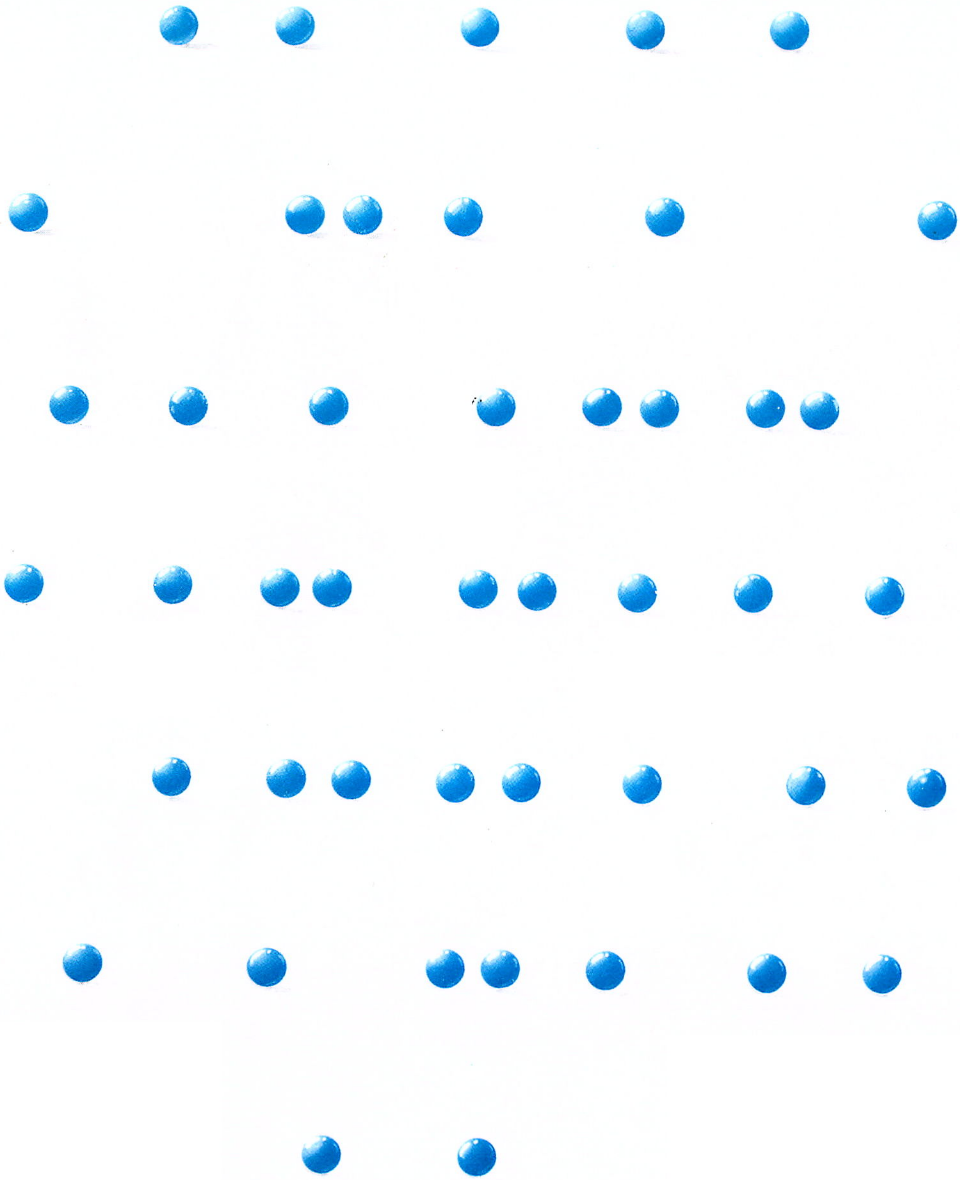
有限群論入門

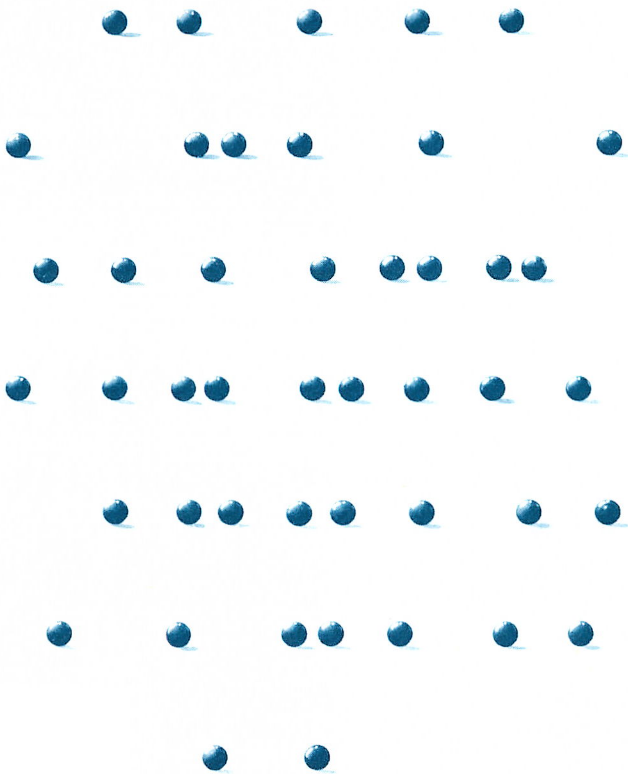
津田塾大学教授 理学博士　森　光弥　著



実教出版株式会社

有限群論入門

津田塾大学教授 理学博士 森 光弥 著



実教出版株式会社

まえがき

本書は著者が津田塾大学数学科で行った講義を加筆・訂正したものである．著者がその講義で目指したことは，有限群論の最も基本的な定理であるシローの定理を紹介し，それまでの道程で習得した群論の基本的な知識によっていくつかの具体的な群の構造を調べることを，学生自らの手で行わせるということであった．純群論的，抽象的な話の連続では内容の消化が不完全になり，目標を見失いがちな学生も，平行して勉強している数学の他の分野――今日では群論の知識はいたるところで必要とされているが，とりわけ整数論や位相幾何学等々――で，群論化された問題にぶつかり，それをどうしても解かなくてはならなくなって苦労しているうちに，群論が少しわかりかけて来たという話を聞いているので，学生にとって手掛けられそうな問題を提供し，問題を解くことによって理論の構成を理解し，また，学生がそれに誘発されて，類似の問題を自分で考えたりできるように心掛けた．以上のことは，そのまま本書の目的とするところである．

群論は抽象的な理論としても興味深いものであるが，初学者にとっては，やや具体的な問題を扱うことを通して定理のデリケートさ，１つ１つの群の個性的な面をはっきりとさせていくのが，勉強していく上にためになると思われる．

説明が冗漫に過ぎたり，また簡単にすぎたりするところが多かったと思われるが，できる限り丁寧に説明するように心掛けた．よりよい理解のために，例題は読んでほしいし，問題も解いてもらいたい．

講義を整理し，一冊の本にするに当って，シローの定理以前の基礎的なところに標準的な内容を取り入れるように心掛けたが，置換群，表現といった多くの重要な項目を落としてしまった．この点については余りしっかりとした考えがあったわけでなく，紙数が増すのをおそれたためである．足りない

ところは巻末にあげた文献によって補ってもらいたい．

文字通り有限群論の入口までしかみちびかなかった著者は，本書の読者が群論に興味をもたれ，さらに進んで下さることを願っている．この本を書くに当って，秋月先生の高等代数学（岩波全書），抽象代数学（基礎数学講座，共立出版）をしばしば参考にした．この2冊の本をさらに読まれるならば，非常に役立つことを確信する．

最後に，この本を書く機会を与えて下さった慶応大学の小野山卓爾教授にここでお礼申し上げたい．また，本書の出版に御尽力いただいた実教出版株式会社の富樫浩氏，橋本正之氏，萩原英一氏その他の方々に厚く感謝の意を表する．

昭和50年8月

著者しるす

目　　次

1章　群の定義と例

2章　部　分　群

3章 準同型・同型

4章 直積・アーベル群・可解群

5章 有限群

1

群の定義と例

1-1 演算の例

群というのは演算が定義されている集合である．はじめに演算という考えを明らかにしておこう．

1-1-1 数の演算

演算といえば，足し算（加法）と掛け算（乗法）を思い浮べる．たとえば，整数についていえば，加法という演算があって，2つの整数 a, b に対して整数 $a+b$ が一通りに定まる．$a+b$ を a と b の**和**という．つぎに，正の有理数全体の集合では乗法という演算があって，2つの正の有理数 a, b に対して**積** $ab>0$ が一通りに定まる．加法も乗法も演算に際して2つの元を用いるので，**2項演算**とよばれる．一般に，1つの集合 M 上の2項演算とは，M の順序のついた2つの元の組 (x, y) に M の元 z を対応させることである．このことを $(x, y)\longmapsto z$ で表す．今後，2項演算を簡単に演算ということにする．

例 1. 自然数の集合 $N=\{1, 2, 3, \cdots\cdots\}$ において，2つの自然数 x, y にその最大公約数 z を対応させること，つまり $(x, y)\longmapsto z$ は演算である．このことを $x*y=z$ で表すと，たとえば，

$$6*8=2, \quad 12*4=4, \quad 3*3=3, \quad 4*7=1$$

例 2. $N'=N\cup\{0\}$ とし，$N'\ni x, y$ に対して，$x+y$ を5で割った余り z を対応させることは演算である．このことを $x\oplus y=z$ で表すならば，たとえば，

$$7\oplus 6=3, \quad 13\oplus 24=2, \quad 14\oplus 6=0, \quad 3\oplus 1=4$$

演算を表すのに，普通の加法，乗法ではそれぞれ＋，×が使われ，上の2つの例では＊とか⊕が用いられたが，演算記号に何を使うかは勝手である．しかし，慣用の記号があれば，それを使うのが普通である．そうでないときは＋とか×，または・，∘などがよく使われるが，＋は後に述べるように使い分けられている．演算 $(x, y)\longmapsto z$ を一般に $x\circ y=z$ で表すことが多い．このとき，z を x と y の**積**または**結合**，**合成**という．

いま，ある集合 A 上の演算がその部分集合 B 上の演算であるかどうかということについて考えてみよう．

例 3.　整数全体の集合 $\boldsymbol{Z}$ 上で，普通の加法は演算である．いま，偶数全体を U とする．2つの偶数を加えた結果はまた偶数であるから，加法は U 上の演算である．このことを，U は加法という演算に関して閉じているという．

一般に，集合 A 上に演算が定義されていて，B は A の部分集合とする．x, y が B の任意の2つの元のとき，$x\circ y$ も B の元であれば，B は**その演算で閉じている**という．

問 1.　つぎの集合は普通の加法で閉じているか．

1）正の偶数全体　　2）奇数全体

問 2.　例1のように，$x*y=x$ と y の最大公約数　とする．つぎの集合は演算 ＊ で閉じているか．

1）　$E=\{1, 2, 3, 4, 5, 6, 7, 8\}$

2）　$F=\{2, 3, 4, 5, 6, 7, 8\}$

3）　$G=\{2, 4, 6, 8\}$

つぎに，演算に際して，$x\circ y$ と $y\circ x$ が同じ元になるかどうかについて考えてみよう．普通の加法について，加法の順序は交換してもかまわない．たとえば，3+5=5+3．同じく普通の乗法においても，たとえば，2×7=7×2 のように，乗法の順序は交換できる．しかし，整数全体の $\boldsymbol{Z}$ 上で，$x\circ y=x-y$（普通の減法）とすれば，たとえば，$5\circ 2=3$，$2\circ 5=-3$ で，$5\circ 2\neq 2\circ 5$．このように演算によっては，$x\circ y$ と $y\circ x$ が同じであるとは限らないから，演算が交換法則をみたす（可換である）かどうかは，それぞれの場合調べな

ければならない.

問 3. 集合 Z で演算 $x \circ y = x + y + 1$ は交換法則をみたすか.

問 4. 正の有理数全体で，つぎの演算は可換であるか.

1) $x \circ y = (x+y)/2$ 2) $x \circ y = 2x + y$

終りに，結合法則について考えてみる．結合法則は，整数全体の集合 Z 上の加法については，任意の3つの整数 x, y, z に対して，

$$(x + y) + z = x + (y + z)$$

が成り立つことであり，正の有理数の集合上の乗法についていえば，3つの正の有理数 x, y, z に対し，つぎの等式の成り立つことをいっている.

$$(x \times y) \times z = x \times (y \times z)$$

しかし，集合 Z 上で，$x \circ y = x - y$ とすれば，たとえば，

$$(8 - 5) - 2 \neq 8 - (5 - 2)$$

演算 $\circ$ に関して結合法則 $(x \circ y) \circ z = x \circ (y \circ z)$ が成り立つときは，両辺ともかっこをつけないで，$x \circ y \circ z$ と書く．たとえば，

$$(x + y) + z = x + (y + z) = x + y + z \text{ である.}$$

問 5. 整数の集合 Z で，つぎの演算は結合法則をみたすか.

1) $x \circ y = x$ 2) $x \circ y = y$ 3) $x \circ y = x + y + 1$

問 6. 正の有理数の集合で，つぎの演算は結合法則をみたすか.

1) $x \circ y = (x + y)/2$ 2) $x \circ y = x \div y$

1-1-2 回転の演算

いままでは，集合として数の集合をとり，演算は算数的であったが，群の元としては回転，移動，写像，関数，記号などもとれ，そのときの演算は四則演算（＋，－，×，÷）のようなものではない．そのような1つの例として，回転の演算を取り上げよう.

正方形の中心（対角線の交点）のまわりの，この正方形がのっている平面上での，正方形をそれ自身に重ねる回転はつぎの4つである．ここで，角度は時計の針の動く向きと反対にはかるとする.

1．　静止（0° の回転）I

2．　90° の回転 a

3．　180° の回転 b

4．　270° の回転 c

いま，90° の回転にひきつづいて 180° の回転を行った結果は 270° の回転であって，このことは回転 a にひきつづいて回転 b を行えば回転 c に等しいことをいい表している．そこで $b\circ a=c$ と定義する．

問 1.　“ひきつづいて行う”という演算で，つぎのことを確かめよ．

$$b\circ c=a,\quad c\circ a=I,\quad a\circ a=b,\quad b\circ b=I,\quad c\circ c=b$$

一般に幾何学的変換では，2つの変換をひきつづき行った結果を2つの変換の組に対応させて，演算を定義する．

1-1-3　写　　像

集合 L, M があって，L の任意の元 a に M の元 a' が唯一つ定まるとき，対応 $a\longmapsto a'$ を L から M への**写像**という．写像 $a\longmapsto a'$ を f で表すとき，a' を a の f による像といい，$f(a)$ で表す：$a'=f(a)$．L から M への写像を $f\colon L\longrightarrow M$ と書くことがある．

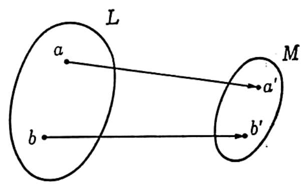


図 1-1

A が L の部分集合のとき，A の元の f による像の全体を A の f による像といい，$f(A)$ と書く：

$$f(A)=\{f(x)|x\in A\}.$$

$f(L)=M$，すなわち，M のどの元も L のどれかの元の像になっているとき，f を L から M の**上への**写像という．

例 1.　$\boldsymbol{R}$ を実数全体の集合とする．任意の実数 x に x^2 を対応させると，$\boldsymbol{R}$ から $\boldsymbol{R}$ への写像 $f\colon \boldsymbol{R}\longrightarrow\boldsymbol{R}$ が得られる．$f(\boldsymbol{R})$ は負でない実数の集合であって，f は上への写像ではない．

例 2.　$g(x)=x+1$ によって，$\boldsymbol{R}$ は $\boldsymbol{R}$ にうつされる．このとき，$g(\boldsymbol{R})=\boldsymbol{R}$ で

ある.

$f(L)\ni b'$ に対して，f によって b' にうつされる L の元の全体を b' の**原像**といい，$f^{-1}(b')$ で表す：$f^{-1}(b')=\{a\in L, f(a)=b'\}$.

$f(L)$ の部分集合 B に対し，f によって B の中にうつされる L の元全体を B の**原像**といい，$f^{-1}(B)$ で表す：

$$f^{-1}(B)=\{x\in L, f(x)\in B\}$$

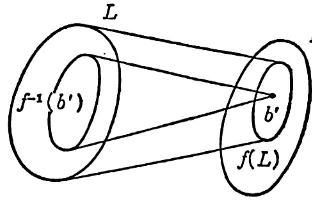


図 1-2

問 1. 例1において，$f^{-1}(x)$ は何個の元からなるか.

問 2. 例2において，$g^{-1}(x)$ は何個の元からなるか.

L の任意の異なる2つの元 a, b に対して，$f(a)\neq f(b)$ であるとき，f は**1対1**であるという.

いま，f が1対1の写像のとき，対応 $x\longmapsto x'=f(x)$ に対して，逆に対応 $x'\longmapsto x$ が考えられる．これを f の**逆写像**といって，f^{-1} で表す：$f(x)=x' \Leftrightarrow x=f^{-1}(x')$．このとき，$f^{-1}$ は $f(L)$ から M の上への1対1写像であり，$(f^{-1})^{-1}=f$ である.

例 3. 例2において，$g(x)=x+1$ の逆写像 g^{-1} は $g^{-1}(x+1)=x$ である．ここで，$x+1$ の代りに x とおけば，$g^{-1}(x)=x-1$ と表される.

集合 M から M 自身の上への1対1写像を M の**変換**または M の上の**置換**という．対応 $x\longmapsto x$ $(x\in M)$ は明らかに M の変換であって，これを M の**恒等変換**または**単位変換**といい，I で表される：$I(x)=x \quad \forall x\in M.$

例 4. 空間（または平面）のすべての点の集合を E^3（または E^2）で表す．その任意の点Pに，Pを一定の方向に一定の距離だけ移動させた点P′を対応させると，E^3（または E^2）の変換が得られる．これを空間（または平面）の**平行移動**という．平行移動は1つのベクトルで表される．すなわち，いまベクトル $\boldsymbol{a}=\overrightarrow{\mathrm{PP'}}$ とすれば，任意の点Qは，平行移動によって，Qからベクトル $\boldsymbol{a}$

を引いたときの終点 Q' にうつされる（図1－3）.

例 5.　空間において，各点を定直線 l のまわりに一定の角 α だけ回転した点にうつせば，E^3 の変換が得られる．これを **l を軸とする回転**といい，α を**回転角**という（図1－4）.

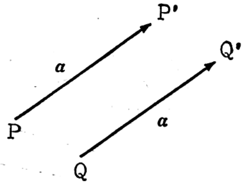


図 1－3

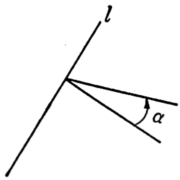


図 1－4

注　l を軸とする回転の回転角は，l の正の方向を定めて，正の方向にネジを進めるとき，ネジのまわる向きに角度をはかるようにすれば，はっきりと定まる.

例 6.　空間において，各点を定平面 π に対称な点にうつすような変換を平面 π に関する**鏡映**(**対称移動**)という（図1－5）.

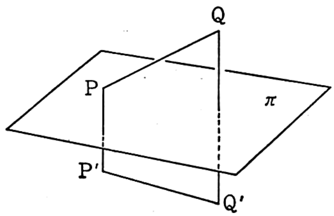


図 1－5

例 7.　平面において，各点を定点 O のまわりに一定の角 α だけ回転した点にうつせば，E^2 の変換が得られる．これを **O を中心とした回転**といい，α をその**回転角**という（図1－6）.

（回転角は時計の針の動く方向と逆の向きを正として符号をつけるのが普通である）

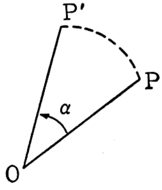


図 1－6

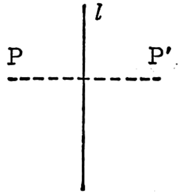


図 1－7

例 8. 平面において，各点を定直線 l に対称な点にうつすような変換を直線 l に関する鏡映（対称移動）という（図 1-7）．これは，この平面を含む空間で考えれば，l を軸とする回転角 180° の回転によって引き起こされる．

1-1-4 写像の積

L, M, N を 3 つの集合とし，f は L から M への，g は M から N への写像とするとき，f, g を続けて行えば，L から N への写像 $a \longmapsto g\ (f(a))$ が得られる：

$$a \overset{f}{\longmapsto} f(a) \overset{g}{\longmapsto} g(f(a))$$

これを f と g の積または結合（合成）といい，gf で表す：

$$gf(a) = g(f(a))$$

例 1. 空間において，ベクトル $\boldsymbol{a}, \boldsymbol{b}$ で表される平行移動をそれぞれ f, g で表せば，積 gf はベクトル $\boldsymbol{a}+\boldsymbol{b}$ で表わされる平行移動である（図 1-8）．

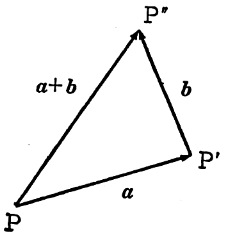


図 1-8

一般に，f, g が集合 M の変換であれば，積 gf も M の変換である．

例 2. 空間において，直線 l を軸とする 2 つの回転を f, g とし，それぞれの回転角を α, β とすれば，積 gf も l を軸とする回転で，その回転角は $\alpha+\beta$ である．

例 3. 空間において，点 O で垂直に交わる直線を OX, OY, OZ とするとき，OX を軸とする 180° の回転を f, OY を軸とする 180° の回転を g とすると，積 gf は OZ を軸とする 180° の回転である（図 1-9）．

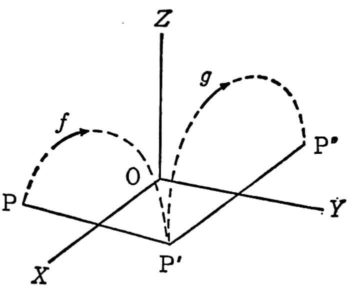


図 1-9

問 1. 上の例で，gf と fg は同じ回

転であることを確かめよ．

問 2. 正方形 ABCD の中心を O とする．O のまわりの，その平面上での 90° の回転 f と，左上から右下にかけての対角線に関する鏡映 g との積 gf は AB, DC の中点を結ぶ直線に関する鏡映であることを確かめよ．また，積 fg はどのような変換か．

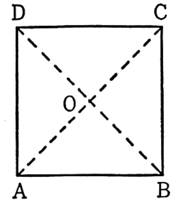


図 1-10

一般に，１つの集合 M の変換 f, g に対して，必ずしも fg と gf は一致しない．

さて，写像の積に関しては，つぎの結合法則が成り立つ．

３つの写像

$$f: L \longrightarrow M, \quad g: M \longrightarrow N, \quad h: N \longrightarrow S$$

に対して

$$h(gf)=(hg)f$$

証明 L の任意の元 x に対して $h(gf)(x)=h(gf(x))=h(g(f(x)))=hg(f(x))=(hg)f(x)$ となるから，L から S への写像として，$h(gf)=(hg)f$．

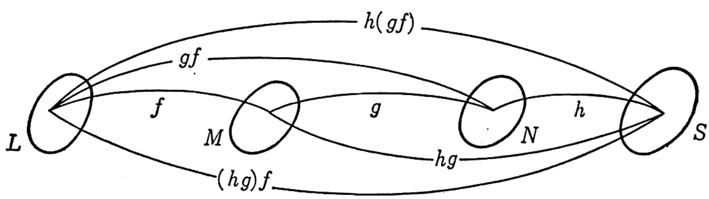


図 1-11

1-2 群 の 定 義

群で定義されている演算は結合法則，単位元の存在，逆元の存在という 3

つの条件をみたしている.

1-2-1 群の定義

いま，正の有理数の全体 $\boldsymbol{Q}^+$ で乗法という演算を考えてみると，つぎのことが成り立っている.

G−1) $\boldsymbol{Q}^+$ の 2 つの元 a, b に対して，その積 $a \times b \in \boldsymbol{Q}^+$

G−2) $\boldsymbol{Q}^+$ の任意の 3 つの元 a, b, c に対して，

$$(a \times b) \times c = a \times (b \times c)$$

G−3) $1 \in \boldsymbol{Q}^+$ であって，$\boldsymbol{Q}^+$ の任意の元 a に対して，

$$1 \times a = a \times 1 = a$$

G−4) $\boldsymbol{Q}^+$ の各元 a に対して，a の逆数 $a^{-1} \in \boldsymbol{Q}^+$ であって，

$$a^{-1} \times a = a \times a^{-1} = 1$$

いま，$\boldsymbol{Q}^+$ の代りに，0 でない有理数の全体 $\boldsymbol{Q}^*$，正の実数全体 $\boldsymbol{R}^+$, 0 でない実数全体 $\boldsymbol{R}^*$， さらに 0 でない複素数全体 $\boldsymbol{C}^*$ をとっても， 上と同じことがいえることは容易にわかる． これら $\boldsymbol{Q}^+$, $\boldsymbol{Q}^*$, $\boldsymbol{R}^+$, $\boldsymbol{R}^*$, $\boldsymbol{C}^*$ が乗法という演算に関してもっている共通の性質を抽象して，つぎのような群の定義が得られる.

[定義] 演算 ∘ が定義されている集合 G において， つぎの条件がみたされているとき，G は**群**をつくる，または，群であるという.

G−1) $G \ni a, b \Longrightarrow$ (ならば) a と b の積 $a \circ b \in G$

G−2) 結合法則：$G \ni a, b, c$ に対して，

$$(a \circ b) \circ c = a \circ (b \circ c)$$

G−3) 単位元の存在：G のすべての元 a に対して，

$$e \circ a = a \circ e = a$$

となるような G の元 e が存在する． この e を G の**単位元**という.

G−4) 逆元の存在：G の各元 a に対して，

$$x \circ a = a \circ x = e$$

となるような G の元 x が存在する． この x を a の**逆元**といい， a^{-1} で表

す（上の 4 つの条件を群の公理ということがある）.

問 1. つぎのおのおのの場合，群のどの公理がみたされないか.

1) すべての有理数全体 $\boldsymbol{Q}$ は乗法に関して群をつくらない.

2) 0 と異なる整数全体は乗法に関して群をつくらない.

問 2. 整数全体の集合 $\boldsymbol{Z}$ で，$x\circ y=x+y+1$ とするとき，つぎのことを示せ.

1) $(x\circ y)\circ z = x\circ(y\circ z)$

2) $(-1)\circ x = x\circ(-1) = x$

3) $(-x-2)\circ x = x\circ(-x-2) = -1$

さて，群 G で単位元 e は唯一つしか存在しない. e' を G の単位元とする. G の任意の元 a に対して，$a\circ e=a$, $e'\circ a=a$ であるから，はじめの式で $a=e'$ とすれば，$e'\circ e=e'$ であり，あとの式で $a=e$ とすれば，$e'\circ e=e$ となり，$e'=e$.

また，群 G の各元 a に対して，逆元 a^{-1} は唯一つしか存在しない. 実際，$x'\circ a=a\circ x'=e$ とすれば，

$$x' = e\circ x' = (a^{-1}\circ a)\circ x' = a^{-1}\circ(a\circ x') = a^{-1}\circ e = a^{-1}$$

[定義]　群 G は，つぎの交換法則が成り立つとき，**可換群**または**アーベル群**という.

G−5)　交換法則：$a\circ b=b\circ a$, 　$\forall a\in G$, $\forall b\in G$

[定義]　群 G は，元の個数が有限のとき，**有限群**といい，その元の個数を G の**位数**といって，記号 $|G|$ で表す. 元の個数が無限な群を**無限群**という.

たとえば，$\boldsymbol{Q}^+$, $\boldsymbol{Q}^*$ は乗法に関して無限アーベル群をつくっている.

1-2-2　群の簡単な性質

(1)　群 G では，$a\circ a=a \Longrightarrow a=e$　(単位元)

$\because$　$e = a^{-1}\circ a = a^{-1}\circ(a\circ a) = (a^{-1}\circ a)\circ a = e\circ a = a$

(2)　群 G では消去律が成り立つ.

$$a\circ b = a\circ c \Longrightarrow b=c, \quad b\circ a = c\circ a \Longrightarrow b=c$$

a の逆元 a^{-1} をそれぞれ左と右からかけてみれば，求める等式を得る．

(3) 群 G の任意の元 a, b に対して，

$$a \circ x = b, \quad y \circ a = b$$

をみたす元 x, y が唯一通りに定まり，$x=a^{-1} \circ b, \quad y=b \circ a^{-1}$

(4) 群 G の任意の元 a, b に対して，$(a \circ b)^{-1}=b^{-1} \circ a^{-1}$

$$\because \quad (a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ (b^{-1} \circ a^{-1}))$$
$$= a \circ ((b \circ b^{-1}) \circ a^{-1}) = a \circ (e \circ a^{-1}) = a \circ a^{-1} = e.$$

同様にして，$(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$ となる．

(5) 群 G の n 個の元 $a_1, a_2, \cdots\cdots, a_n$ に対して，

$$(a_1 \circ a_2 \circ \cdots\cdots \circ a_n)^{-1} = a_n{}^{-1} \circ a_{n-1}{}^{-1} \circ \cdots\cdots \circ a_2{}^{-1} \circ a_1{}^{-1}$$

問 1. 群 G の元 a について $(a^{-1})^{-1}=a$ となることを説明せよ．

例題 1. 群 G の任意の元 x について，$x \circ x=e$ であれば，G はアーベル群である．

証明 $x \circ x=e$ の両辺に左から x^{-1} をかければ，$x=x^{-1}$ となる．いま G の任意の元 a, b に対し，$a \circ b=(a \circ b)^{-1}=b^{-1} \circ a^{-1}=b \circ a$ となるから，G はアーベル群である．

注 群 G の3つの元 a_1, a_2, a_3 に対し，$(a_1 \circ a_2) \circ a_3$ を3つの元 a_1, a_2, a_3 の積といって $a_1 \circ a_2 \circ a_3$ で表す．結合法則により，$(a_1 \circ a_2) \circ a_3=a_1 \circ (a_2 \circ a_3)$ で，かっこのつけ方に関係がないから，かっこをつけないわけである．そこで，群 G で，

$$(a_1 \circ a_2) \circ a_3 = a_1 \circ a_2 \circ a_3$$
$$(a_1 \circ a_2 \circ a_3) \circ a_4 = a_1 \circ a_2 \circ a_3 \circ a_4$$

一般に，

$$(a_1 \circ a_2 \circ \cdots\cdots \circ a_{n-1}) \circ a_n = a_1 \circ a_2 \circ \cdots\cdots \circ a_{n-1} \circ a_n$$

と定義する．そうすると，つぎの式が成り立つ．

$$(a_1 \circ a_2 \circ \cdots\cdots \circ a_n) \circ (a_{n+1} \circ \cdots\cdots \circ a_m) = a_1 \circ a_2 \circ \cdots\cdots \circ a_m$$

証明 $m=3$ のときは，結合法則と3つの元の積の定義から，上の式は成り立つ．$3<m$ とし，m より小さい数については上の式が成り立つと仮定し，帰納法で証明する．

$$\text{左辺} = (a_1 \circ a_2 \circ \cdots\cdots \circ a_n) \circ ((a_{n+1} \circ \cdots\cdots \circ a_{m-1}) \circ a_m) \qquad (\text{定義})$$

$$= ((a_1 \circ a_2 \circ \cdots\cdots \circ a_n) \circ (a_{n+1} \circ \cdots\cdots \circ a_{m-1})) \circ a_m \quad \text{(結合法則)}$$

$$= (a_1 \circ a_2 \circ \cdots\cdots \circ a_{m-1}) \circ a_m \quad \text{(帰納法の仮定)}$$

$$= a_1 \circ a_2 \circ \cdots\cdots \circ a_m \quad \text{(定義)}$$

たとえば，$(a_1 \circ a_2 \circ a_3) \circ (a_4 \circ a_5) = a_1 \circ a_2 \circ a_3 \circ a_4 \circ a_5$,

$$((a_1 \circ (a_2 \circ a_3)) \circ (a_4 \circ a_5)) \circ a_6$$
$$= ((a_1 \circ a_2 \circ a_3) \circ (a_4 \circ a_5)) \circ a_6$$
$$= (a_1 \circ a_2 \circ a_3 \circ a_4 \circ a_5) \circ a_6$$
$$= a_1 \circ a_2 \circ a_3 \circ a_4 \circ a_5 \circ a_6$$

3個以上の元の演算で，かっこをどのようにつけても一定の結果が得られるわけで，したがって，かっこをつける必要がないことになる．

注　群 G がアーベル群のとき，G の3個以上の元の積も，その演算の順序に関係ない．すなわち，$a_1, a_2, \cdots\cdots, a_n$ の順序をどんなにかえて $a_{p_1}, a_{p_2}, \cdots\cdots, a_{p_n}$ をつくっても，

$$a_1 \circ a_2 \circ \cdots\cdots \circ a_n = a_{p_1} \circ a_{p_2} \circ \cdots\cdots \circ a_{p_n}$$

証明　$n=2$ なら，上式は交換法則にほかならない．$n-1$ 個の元については成り立つと仮定して，n 個の元について証明する．左辺から，$a_i \circ a_{i+1} = a_{i+1} \circ a_i$ という操作を反復使って，a_{p_n} を一番終りにもっていくと，$a_1 \circ a_2 \circ \cdots\cdots \circ a_n = a_1 \circ \cdots\cdots \circ a_n \circ a_{p_n}$. さて，$a_{p_1} \circ \cdots\cdots \circ a_{p_{n-1}}$ は，この式の右辺のはじめの $n-1$ 個の元の積 $a_1 \circ \cdots\cdots \circ a_n$ の順序をかえたものであるから，帰納法の仮定によりこれら2つは等しい．したがって，

$$a_1 \circ a_2 \circ \cdots\cdots \circ a_n = a_{p_1} \circ a_{p_2} \circ \cdots\cdots \circ a_{p_n}$$

1-2-3　群の公理について

先に述べた群の公理 G−1), −2), −3), −4) を出発点として，これから理論を展開していくわけである．ちょうど，ユークリッド幾何学において，平行線の公理や合同の公理から，いろいろな図形に関する定理がみちびかれるのと同じである．公理は具体的な例からその本質的な事柄を抽象して整理したもので，これからみちびかれる理論は個々の具体例に適用できるという普遍性をもっている．

いま，ここで，先のものより簡単な群の公理系について述べる．

[定理 1] 演算が定義されている集合 G において，つぎの条件がみたされていれば，G は群をつくる．

G−1) $G \ni a, b \Longrightarrow a \circ b \in G$

G−2) 結合法則：$G \ni a, b, c$ に対して，

$$(a \circ b) \circ c = a \circ (b \circ c)$$

G−3′) 左単位元の存在：G のすべての元 a に対して，

$$e \circ a = a$$

となるような G の元 e（左単位元）が存在する．

G−4′) 左逆元の存在：G の各元 a に対して，

$$x \circ a = e$$

となるような G の元 x（左逆元）が存在する．

[証明] まず，$G \ni a$ に対して G−4′) で述べた x，すなわち $x \circ a = e$ となる x をとる．G−4′) より $y \circ x = e$ となる y が存在する．まず，

$$\begin{aligned} a \circ x &= (e \circ a) \circ x = ((y \circ x) \circ a) \circ x \\ &= (y \circ (x \circ a)) \circ x = (y \circ e) \circ x = y \circ (e \circ x) \\ &= y \circ x = e. \end{aligned}$$

さて，$a \circ e = a \circ (x \circ a) = (a \circ x) \circ a = e \circ a = a$ が成り立つ．したがって，e は単位元，x は逆元である．よって，G は群をつくる．

G−1)，−2)，−3)，−4) が成り立てば，G−1)，−2)，−3′)，−4′) は明らかに成り立つが，上に示したように G−1)，−2)，−3′)，−4′) から G−1)，−2)，−3)，−4) がみちびかれるから，これら 2 つの公理系は同値である．互いに同値な公理系からはもちろん同じ理論が得られる．

問 1. 群の定義において，G−3)，−4) の代りに，つぎの 2 つを公理としてとってよいことを確かめよ．

G−3″) 右単位元の存在：G のすべての元 a に対して，

$$a \circ e = a$$

となるような G の元 e（右単位元）が存在する．

G−4″) 右逆元の存在：G の各元 a に対して，

$$a \circ x = e$$

となるような G の元 x（右逆元）が存在する．

例題 1.　演算が定義されている集合において，G−1)，−2) が成り立ち，さらに，逆の演算が可能であるとき，すなわち，

G−5)　　G の任意の元 a, b に対して，

$$a \circ x = b, \qquad y \circ a = b$$

となる G の元 x, y が存在すれば，G は群をつくる．

証明　G の1つの元 c を定める．まず，$e \circ c = c$ となる解 e が存在する．G の任意の元 a に対し，$c \circ y = a$ となる y がとれ，$(e \circ c) \circ y = c \circ y$．左辺を書きかえて，$e \circ (c \circ y) = e \circ a$，すなわち，$e \circ a = a$，したがって，G−3′) が成り立つ．

つぎに，a と e に対し，$x \circ a = e$ となる x がとれるから，G−4′) が成り立つ．したがって，G は群をつくる．

1-2-4　乗法群と加法群[1)]

群の2つの元 a, b の積を表すのに，場合に応じて $a \circ b$, $a \cdot b$, $a \times b$, $a + b$ などいろいろあるが，群の演算記号に乗法記号 ab がよく使われる．演算が乗法記号で示された群を**乗法群**という．乗法群では元 a の逆元を a^{-1} で表す．単位元は1で表されることがある．

(1)　<u>元の累(巾)乗</u>　　乗法群 G では，元 a の n 個の積 $\overbrace{aa\cdots\cdots a}^{n}$ を簡単に a^n で表す．とくに $a^1 = a$ である．

このとき，任意の自然数 m, n に対して，つぎの等式が成り立つ：

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn} \tag{1-1}$$

$$ab = ba \text{ であれば} \qquad (ab)^m = a^m b^m \tag{1-2}$$

つぎに，$(a_1 a_2 \cdots\cdots a_n)^{-1} = a_n^{-1} \cdots\cdots a_2^{-1} a_1^{-1}$ であるから，$(a^n)^{-1} = (a^{-1})^n$ (n は正の整数）となる．いま，

$$a^0 = 1 \text{（単位元）}, \qquad a^{-n} = (a^n)^{-1}$$

と定義する．そうすれば，m, n が正，負の整数または0のとき，

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn} \tag{1-3}$$

が成り立ち，また，$ab = ba$ であれば，

$$(ab)^m = a^m b^m \tag{1-4}$$

1)　付録1参照．

アーベル群では演算記号として加法の記号を用い，元 a と元 b の結合を $a+b$ で表すことが多い．このとき $a+b$ を a と b の**和**という．演算が加法記号で表されたアーベル群を**加法群**または**加群**という．

加法群では単位元を $\mathbf{0}$ で表し，**零元**という．$\mathbf{0}$ は $a+\mathbf{0}=a$ によって一意的に定まる元である．また元 a の逆元，すなわち，$a+x=\mathbf{0}$ となる元 x を $-a$（マイナス a）で表す．したがって，

$$a+(-a)=(-a)+a=\mathbf{0}$$

$a+(-b)$ のことを $a-b$ と書き，a から b を引いた**差**という．$a-b$ は $x+b=a$ の解である．逆元の性質から，

$$-(-a)=a, \quad -(a+b)=-a-b, \quad -(a-b)=-a+b$$

(2) 元の n 倍　加法群の元 a を n 個加えた和 $\overbrace{a+a+\cdots\cdots a}^{n}$ を na で表す．とくに $1\cdot a=a$.

$$-(a_1+a_2+\cdots\cdots+a_n)=-a_1-a_2-\cdots\cdots-a_n$$

であるから，$-(na)=n(-a)$（n は正の整数）となる．いま，

$$0a=\mathbf{0}\ (\text{零元}), \quad (-n)a=-na$$

と定義する．たとえば，$(-3)a=-(3a)=3(-a)$．ここで，a は数とは限らないから，$(-3)a$ は -3 と a の積を意味するとは限らない．

乗法群の場合の（1-3），（1-4）に対応して，つぎの式が成り立つ．

m, n が正，負の整数または 0 のとき，

$$(m+n)a=ma+na, \quad m(na)=(mn)a \qquad (1\text{-}5)$$

$$m(a+b)=ma+mb \qquad (1\text{-}6)$$

注　今後，加法群の零元 $\mathbf{0}$ を簡単に数字の 0 で表すことがある．

1-3 群 の 例

(1) 数の乗法群　つぎの各集合はふつうの乗法で群をつくる．

1) 正の有理数全体 $\boldsymbol{Q}^+$，正の実数全体 $\boldsymbol{R}^+$

2) 0 でない有理数全体 $\boldsymbol{Q}^*$， 0 でない実数全体 $\boldsymbol{R}^*$， 0 でない複素数全

体 $\boldsymbol{C}^*$

3)　$\{z \mid z \in \boldsymbol{C},\ |z| = 1\}$

(2)　**数の加法群**　　つぎの各集合はふつうの加法で群をつくる．

整数全体 $\boldsymbol{Z}$,　有理数全体 $\boldsymbol{Q}$,　実数全体 $\boldsymbol{R}$,　複素数全体 $\boldsymbol{C}$

以上の群はすべて無限群である．

(3)　$\{1, -1, i, -i\}$，i は虚数単位$\sqrt{-1}$，は 4 個の元からなる，すなわち位数 4 の乗法群をつくる．

(4)　集合 M から M 自身の上への 1 対 1 写像を M の変換という(1-1-3 項)．φ, ψ が M の変換であれば，積 $\psi\varphi$ も M の変換である．φ, ψ, ρ が M の変換であれば，結合法則 $\rho(\psi\varphi)=(\rho\psi)\varphi$ は成り立つ．

対応 $x \longmapsto x$ $(\forall x \in M)$ は M の変換で，恒等変換とよばれ，I で表される：$I(x)=x \quad \forall x \in M$．$\varphi$ を M の変換とすれば，$I(\varphi(x))=\varphi(x) \quad \forall x \in M$，よって $I\varphi=\varphi$．また φ は M から M の上への 1 対 1 写像であるから，逆写像 φ^{-1} が考えられる．φ^{-1} は M の変換であって，$\varphi^{-1}\varphi(x)=x \quad \forall x \in M$ であるから，$\varphi^{-1}\varphi=I$．以上まとめると，

[定理 2]　　集合 M の変換の全体を S^M とする．S^M は変換の積に関して群をつくる．これを M の**変換群**という．単位元は恒等変換 I: $x \longmapsto x$ であり，変換 φ: $x \longmapsto x'$ の逆元は逆変換 φ^{-1}: $x' \longmapsto x$ である．

$$I\varphi = \varphi I = \varphi \quad \forall \varphi \in S^M, \qquad \varphi^{-1}\varphi = \varphi\varphi^{-1} = I \quad \forall \varphi \in S^M$$

(5)　***n* 次対称群 $\mathfrak{S}_n$**　　M が有限集合のとき，M の元に番号 1, 2, ……n をつけて，この番号によって M の元を示すことができる．さて，$i \longmapsto p_i$ $(i=1, 2, \cdots\cdots, n)$ という置換を，

$$\begin{pmatrix} 1 & 2 \cdots\cdots & n \\ p_1 & p_2 \cdots\cdots & p_n \end{pmatrix}$$

で示す．この記法では上下の組だけが問題で，たとえば，$n=3$ のとき，

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$$

であって，これらはすべて $M=\{1, 2, 3\}$ の上の，$1\longmapsto 3$, $2\longmapsto 1$, $3\longmapsto 2$ という置換である．

置換 σ によって $i\longmapsto p_i$，置換 τ によって $p_i\longmapsto q_i$ であるとき，積 $\tau\sigma$ は $i\longmapsto q_i$ という置換である．たとえば，$n=3$ のとき，

$$\sigma=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\qquad \tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

とすれば，

$$\sigma\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&3&2\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$\tau\sigma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}2&3&1\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

この例が示すように，置換の積では交換法則は成り立つとは限らない．

M の各文字をそれ自身にうつす置換

$$e=\begin{pmatrix}1&2\cdots\cdots n\\1&2\cdots\cdots n\end{pmatrix}$$

が単位置換であり，また置換 σ: $i\longmapsto p_i$

$$\sigma=\begin{pmatrix}1&2\cdots\cdots n\\p_1&p_2\ \cdots\ p_n\end{pmatrix}$$

の逆置換 σ^{-1} は σ^{-1}: $p_i\longmapsto i$ であるから，

$$\sigma^{-1}=\begin{pmatrix}p_1&p_2\cdots\cdots p_n\\1&2\cdots\cdots\ n\end{pmatrix}$$

問 1. つぎの σ, τ について，$\sigma\tau$, $\tau\sigma$ および σ^{-1}, τ^{-1} を求めよ．

$$\sigma=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\qquad \tau=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$$

$M=\{1, 2, \cdots\cdots, n\}$ の置換の全体は定理 2 で述べたように，1つの群 S^M をつくる．これを n 次対称群といって，$\mathfrak{S}_n$ で表す．$\mathfrak{S}_n$ の元と $1, 2\cdots\cdots, n$ の順列とは1対1に対応するから，$\mathfrak{S}_n$ の位数は順列の個数 $n!$ に等しい．

(6) 幾何学的変換群

(a) **合同変換群**　空間のすべての点の集合を E^3 とする．E^3 の変換は，任意の2点 P, Q の距離と，P, Q の像 P′, Q′ の距離が等しいとき，**合同変換**とよばれる．回転，平行移動，平面に関する鏡映は特別な合同変換である．一般の合同変換はこれら3種の変換をいくつかひきつづいて行った結果，すなわち積として得られる．

合同変換全体は E^3 の**合同変換群**[1] とよばれる群をつくる．

［証明］ 結合法則は成り立つ．いま，φ, ϕ を合同変換，P, Q を E^3 の任意の2点とし，$\mathrm{P} \overset{\varphi}{\longmapsto} \mathrm{P}' \overset{\phi}{\longmapsto} \mathrm{P}''$, $\mathrm{Q} \overset{\varphi}{\longmapsto} \mathrm{Q}' \overset{\phi}{\longmapsto} \mathrm{Q}''$ とすれば，$\mathrm{P}''\mathrm{Q}''=\mathrm{P}'\mathrm{Q}'=\mathrm{PQ}$．したがって，$\phi\varphi$ も合同変換である．恒等変換は明らかに合同変換である．つぎに合同変換 φ の逆変換 φ^{-1} について，$\mathrm{P}' \overset{\varphi^{-1}}{\longmapsto} \mathrm{P}$, $\mathrm{Q}' \overset{\varphi^{-1}}{\longmapsto} \mathrm{Q}$ のとき，$\mathrm{P} \overset{\varphi}{\longmapsto} \mathrm{P}'$, $\mathrm{Q} \overset{\varphi}{\longmapsto} \mathrm{Q}'$ であるから，$\mathrm{P}'\mathrm{Q}'=\mathrm{PQ}$．したがって，$\varphi^{-1}$ も合同変換である．

(b) **回転群**　定点Oを通る直線を回転軸とする2つの回転の積は，またOを通る直線を回転軸とする1つの回転である．定点Oを通る直線を回転軸とする回転の全体は，**Oのまわりの回転群**とよばれる群をつくっている．

注　E^3 の合同変換はいくつかの，平面に関する鏡映の積として表される．このとき，積に現れる鏡映が偶数個か奇数個かは，表し方に関係しない．偶数個の鏡映の積である合同変換は向きを変えない変換で，**変位**または**運動**とよばれる．奇数個の鏡映の積である合同変換は向きを変える変換である．

変位は平行移動か，回転か，あるいは回転のあとに，回転軸に沿って平行移動を行ったものである．定義によって，2つの変位の積はまた変位である．1つの鏡映の逆変換はその鏡映自身であるから，変位の逆変換は変位である．恒等置換は1つの鏡映を2回ひきつづき行ったものであるから，変位である．したがって，変位の全体は，E^3 の**変位群**または**運動群**とよばれる群をつくっている．

向きを変える合同変換は平行移動のあとで，その移動の方向に平行な1つの平面に関する鏡映を行ったものか，回転にひきつづいて，その回転軸に垂直な1つの平面に関する鏡映を行ったものである．

1）巻末文献〔21〕参照．

このように，E^3 の合同変換は平行移動と回転と鏡映とから合成されているので，E^3 の合同変換群は平行移動，回転，鏡映で**生成されている**という．また，上に示したように，E^3 の変位群は平行移動と回転で生成されている．

1点Oを動かさない合同変換は，それが変位であれば，Oを通る直線を軸とする回転であり，変位でなければ，回転にひきつづいて，Oを通る1つの平面に関する鏡映を行ったものである．したがって，Oを通る直線を軸とする回転の積はまたOを通る直線を軸とする回転であって，Oを通る直線を軸とする回転だけが集まって1つの群（p. 18，(b) で述べたOのまわりの回転群）をつくっている．

E^3 の平行移動の積はまた平行移動であり，平行移動の全体は，**平行移動群**とよばれる群をつくっている．

しかし，鏡映は，それだけが集まって1つの群をつくることはない．なぜなら，2つの鏡映の積は，容易にわかるように，対称面が平行であれば，平行移動であり，平行でなければ，2つの面の交線を軸とする回転になるからである．

鏡映の積の全体をとれば，それは群になり，その群は E^3 の合同変換群にほかならず，また偶数個の鏡映の積の全体も1つの群をつくり，それは E^3 の変位群である．

(c) **3次の2面体群 D_3** 　正三角形をそれ自身に重ねる E^3 の回転について考えてみよう．正三角形の中心（つまり重心）Oは，これらの回転によって動かないから，Oを通る直線を軸とする回転で，正三角形をそれ自身にうつすものを求めればよい．まず，Oを通って正三角形に垂直な直線を軸とする回転は，回転角 0° の恒等変換 e，回転角 120° の回転 σ，回転角 240° の回転 σ^2 の3つである．

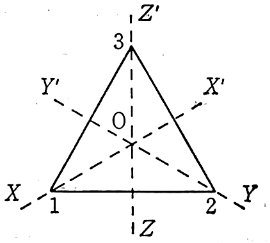


図 1-12

また，正三角形ののっている平面上の直線を軸とする回転は，左下から右上にかけての対称軸 XX'，右下から左上にかけての対称軸 YY'，真下から真

上にかけての対称軸 ZZ' を軸とする 180° の回転 τ_1, τ_2, τ_3 の3つある．以上6個の回転が正三角形をそれ自身に重ねる回転全体で，これらは1つの群をつくっている．なぜなら，結合法則は明らかに成り立ち，恒等変換は単位元になっている．λ, μ を6個の回転からとれば，$\lambda\mu$ もOのまわりの回転で，正三角形をそれ自身に重ねるから，6個の回転のどれかと一致する．また，λ を6個の回転のどれかとすれば，λ の逆変換 λ^{-1} も6個の回転のいずれか1つになっている．たとえば，σ^{-1} は-120° の，つまり 240° の回転 σ^2 であり，各 τ_i の逆は τ_i である．この群を3次の2面体群といい，D_3 で表す．

問 2． 正方形をそれ自身に重ねる回転は8個あって，全体で1つの群（4次の2面体群とよばれ，D_4 で表される）をつくることを示せ．

(d) **クラインの４元群**　長方形（正方形でない）の対称軸 XX' に関する鏡映を σ，対称軸 YY' に関する鏡映を τ とすると，積 $\tau\sigma$ は中心Oを通り長方形に垂直な直線を軸とする 180° の回転 ρ に等しい（p.7，例3)．さて，

$$\sigma^2 = \tau^2 = \rho^2 = e \quad (\text{恒等変換})$$

であり，$\sigma\tau = \tau\sigma = \rho$ であることは容易に確かめられる．したがって，

$$\sigma\rho = \rho\sigma = \tau, \quad \tau\rho = \rho\tau = \sigma$$

となるので，交換法則が成り立ち，

$$\{e, \sigma, \tau, \rho\}$$

は4つの元からなるアーベル群である．

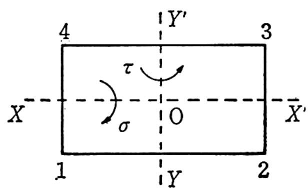


図 1-13

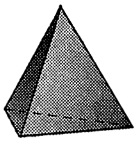
これは長方形をそれ自身に重ねる E^3 の回転のつくる群である．この群を**クラインの4元群**という．

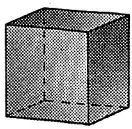
(7) **多面体群**[1)]　正多面体には正4面体，正6面体，正8面体，正12面

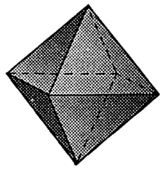
1)　巻末文献〔21〕参照．

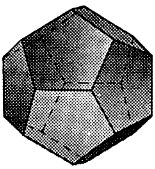
体，正 20 面体の 5 種類しかないことがわかっている．

正 6 面体（立方体）のおのおのの面の中心を結べば，内接する正 8 面体が得られ（図 1－15），逆に正 8 面体のおのおのの面の中心を結べば，内接する


正4面体


正6面体


正8面体


正12面体

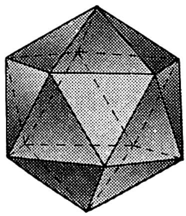
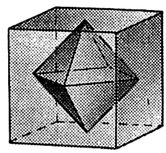

正20面体

図 1－14


図1－15

正 6 面体が得られる． 同様に， 正 12 面体のおのおのの面の中心を結べば，正 20 面体が得られ， 逆に正 20 面体のおのおのの面の中心を結べば， 正 12 面体が得られる．正 6 面体と正 8 面体，正 12 面体と正 20 面体はそれぞれ互いに双対的であるといわれる．

はじめに正 4 面体をそれ自身に重ねる回転について考えてみよう． そのような回転はつぎの 2 種類である．

(1) 頂点とその対面の中心を結ぶ直線を軸とする回転

(2) 向い合う 2 つの辺の中点を結ぶ直線を軸とする回転

(1) の種類の対称軸は 4 本あって，それぞれを軸とする，恒等変換でない回転は 2 つずつある．(2) の種類の対称軸は 3 本あって，それぞれを軸とする，恒等変換でない回転は 1 つずつある．したがって，正 4 面体をそれ自身に重ねる回転は全部で，$1+2\times4+1\times3=12$ 個ある．

一般に正多面体 V の中心 O のまわりの回転で，V をそれ自身に重ねる回転の全体 G は，1つの群をつくる．G では結合法則が成り立ち，恒等変換 $e \in G$ である．いま，$G \ni \sigma, \tau$ とすれば，$\sigma\tau$ も V を V 自身に重ねる回転であるから，$\sigma\tau \in G$．また $G \ni \sigma$ のとき，σ の回転軸と，その上にない頂点とで定まる平面に関して V は面対称であるから，σ の逆変換 σ^{-1} によって V は V 自身に重なる．したがって $\sigma^{-1} \in G$．

正多面体の中心 O のまわりの，その正多面体をそれ自身に重ねる回転のつくる群を，正多面体が正 4 面体，正 6 面体，正 8 面体，正 12 面体，正 20 面体であるにしたがって，それぞれ **正 4 面体群**，**正 6 面体群**，**正 8 面体群**，**正 12 面体群**，**正 20 面体群** という．先に述べたように，正 6 面体をそれ自身に重ねる回転は正 8 面体をそれ自身に重ねる回転であり，正 12 面体をそれ自身に重ねる回転は正 20 面体をそれ自身に重ねる回転であるから，正 6 面体群と正 8 面体群は一致し，正 12 面体群と正 20 面体群は一致する．

多面体群がおのおのの場合いくつの元からなるか調べてみよう．

多面体群の回転の軸，つまり正多面体の対称軸にはつぎの種類がある．

（i）　向かい合った頂点を結ぶ直線

（ii）　向かい合った面の中心を結ぶ直線

（iii）　向かい合った頂点と面の中心を結ぶ直線

（iv）　向かい合った辺の中点を結ぶ直線

対称軸の総数を n とし，（i），(ii)，(iii)，(iv) の種類のものの個数をそれぞれ n_1, n_2, n_3, n_4 とすれば表 1-1 のようになる．

表 1-1

	n_1	n_2	n_3	n_4	n
正 4 面体	0	0	4	3	7
正 6 面体	4	3	0	6	13
正 8 面体	3	4	0	6	13
正 12 面体	10	6	0	15	31
正 20 面体	6	10	0	15	31

さて，（i）の種類の対称軸を軸とする回転の個数は，その軸上の1つの頂点に集まる辺の個数 p_1 に等しい．(ii)，(iii) の種類の1つの対称軸を軸と

する回転の個数は，1つの面の頂点の個数 p_2 に等しい．(iv) の種類の対称軸を軸とする回転は恒等変換と回転角 180° の回転の2つである．したがって (i)〜(iv) の種類のうち1つの対称軸を軸とする回転の個数は，恒等変換を除けば，それぞれ，p_1-1, p_2-1, p_2-1, 1 であって，したがって，回転の総数

表 1-2

	p_1	p_2	N
正 4 面体	3	3	12
正 6 面体	3	4	24
正 8 面体	4	3	24
正 12 面体	3	5	60
正 20 面体	5	3	60

$$N = n_1(p_1-1)+n_2(p_2-1)$$
$$+n_3(p_2-1)+n_4+1$$
$$=n_1(p_1-1)+(n_2+n_3)(p_2-1)+n_4+1$$

で，各多面体群について求めれば，表1-2のようになる．

(8) **n 次2面体群 D_n**[1]　先に述べた3次2面体群を一般化しよう．平面上の正 n 角形 W を空間図形とみて，その中心Oのまわりの回転で，W を W に重ねるものの全体を考えてみると，これらは1つの群をつくる．これを n 次の2面体群といって，D_n で表す．

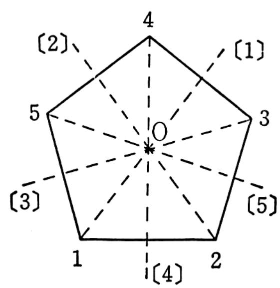


図 1-16

D_n の回転軸はつぎの4種類ある．

(i) 中心Oを通り，正 n 角形 W に垂直な直線

(ii) 向かい合う頂点を結ぶ直線

(iii) 向かい合う辺の中点を結ぶ直線

(iv) 向かい合う頂点と辺の中点を結ぶ直線

(i) の種類の回転軸をもつ回転は恒等変換 e と，回転角 $2\pi/n$ の回転 σ の巾である $\sigma, \sigma^2, \cdots\cdots, \sigma^{n-1}$ の n 個ある．

n が偶数であれば，(ii), (iii) の種類の対称軸はそれぞれ $n/2$ 本ずつあ

1) 巻末文献〔21〕参照．

り，n が奇数ならば，(iv) の種類の対称軸が n 本ある．いずれの場合にも，それぞれの対称軸を軸とする回転は恒等変換を除けば，回転角 180° の回転唯一つである．したがって，D_n の元の個数，つまり位数は $2n$ である．

問 3.　図1-16において，中心Oと頂点 k を結ぶ直線を〔k〕で表すことにする．いま τ は〔2〕を軸とする 180° の回転とするとき，つぎのことを確かめよ．

1) $\tau\sigma$ は軸〔4〕に関する鏡映である．　2) $\tau\sigma^2$ は軸〔1〕に関する鏡映である．　3) $\tau\sigma^3$ は軸〔3〕に関する鏡映である．　4) $\tau\sigma^3$ は軸〔5〕に関する鏡映である．　5) $\sigma^5=e$, $\tau^2=e$, $\sigma\tau=\tau\sigma^4$ が成り立つ（e は恒等置換）．

上の問からわかるように，5次の2面体群は，(iv) の種類の1つの対称軸に関する鏡映を τ とすれば，

$$e,\ \sigma,\ \sigma^2,\ \sigma^3,\ \sigma^4,\ \tau,\ \tau\sigma,\ \tau\sigma^2,\ \tau\sigma^3,\ \tau\sigma^4$$

の10個の元からなっていて，σ, τ は，

$$\text{関係}\quad \sigma^5=e,\ \tau^2=e,\ \sigma\tau=\tau\sigma^4$$

をみたしている．

この事実を，D_5 は，$\sigma^5=\tau^2=e$, $\sigma\tau=\tau\sigma^4$ をみたす2つの元 σ, τ で生成されているという．

一般に，n 次の2面体群 D_n は，(i) の種類の対称軸のまわりの回転角 $2\pi/n$ の回転を σ，(i) 以外の種類の1つの対称軸に関する鏡映を τ とすれば，

$$e,\ \sigma,\ \sigma^2,\ \cdots\cdots,\ \sigma^{n-1},\qquad \tau,\ \tau\sigma,\ \cdots\cdots,\ \tau\sigma^{n-1} \tag{☆}$$

の $2n$ 個の元から成っている．また，σ, τ はつぎの関係をみたしている：

$$\sigma^n=e,\ \tau^2=e,\ \sigma\tau=\tau\sigma^{n-1} \tag{☆☆}$$

問 4.　3次の2面体 D_3，4次の2面体 D_4，6次の2面体 D_6 について，上述のことを確かめよ．また (☆☆) より $\sigma^i\tau=\tau\sigma^{n-i}$ をみちびけ．

注　E^3 において，定点Oのまわりの回転のつくる有限群は，つぎの種類のものしかないことが知られている[1]．

1)　1つの軸のまわりの回転角 $2\pi/n$ の回転 σ の巾からなる

群　$\{e,\ \sigma,\ \sigma^2,\ \cdots\cdots,\ \sigma^{n-1}\}$

---

1)　巻末文献〔8〕〔21〕参照．

2) クラインの4元群．これは長方形をそれ自身に重ねる中心Oのまわりの回転のつくる，位数4のアーベル群（(6) の (d)).

3) n 次2面体群 D_n ($n\geqq 3$)

4) 正 n 面体群（ここで $n=4, 8, 20$）

注 クラインの4元群は，$n=2$ としたときの (☆)，(☆☆) をみたしている．

(9) **巡回群** 群 G の各元が1つの元 a の巾になっているとき，G を a で生成された**巡回群**といい，$\langle a\rangle$ で表し，a を巡回群の**生成元**という．$a^m a^n = a^{m+n} = a^n a^m$ であるから，巡回群はアーベル群である．

i) i と j が異なるとき，a^i と a^j が異なるならば，$G=\langle a\rangle$ は，

$$\cdots\cdots a^{-2}, a^{-1}, a^0=e, a, a^2, \cdots\cdots$$

からなる無限群である．

ii) そうでないときは，$a^h=a^k (h>k)$ となる h, k が存在する．したがって，$a^{h-k}=e, h-k>0$ となる．いま，n を $a^n=e$ となる最小の正整数とすれば，$a^0=e, a, a^2, \cdots\cdots, a^{n-1}$ は互いに異なる．i を任意の整数とするとき，$i=nq+r, 0\leqq r<n$, となる整数 q, r が存在するから，$a^i=a^{nq+r}=(a^n)^q a^r = ea^r=a^r$ となる．したがって，a の巾は $e, a, a^2, \cdots\cdots, a^{n-1}$ のどれかと一致する．$a^i=e$ となるのは，i が n で割り切れるとき，またそのときに限る．以上まとめて，

[定理 3] 巡回群 $G=\langle a\rangle$ において，$a^m=e$ をみたす自然数 m が存在すれば，G は有限巡回群である．n をこのような m のうちの最小自然数とすれば，G は，

$$a^0=e, a, a^2, \cdots\cdots, a^{n-1}$$

の n 個の元からなる．また $a^h=e \Leftrightarrow h$ が n の倍数．

[定義] 群 G の元 a に対し，$a^m=e$ となる自然数 m が存在するとき，m の最小値を a の**位数**という．したがって，有限巡回群 $\langle a\rangle$ の位数は生成元の位数に等しい．

1-4 置換の分解

集合 $M=\{1, 2, \cdots\cdots, n\}$ の置換，つまり n 次対称群 $\mathfrak{S}_n$ の元を特別な形の置換の積に分解することを考える．

M に属する $\alpha_1, \alpha_2, \cdots\cdots, \alpha_r$ を $\alpha_1 \longmapsto \alpha_2 \longmapsto \cdots\cdots \longmapsto \alpha_r \longmapsto \alpha_1$ と巡回的にうつし，他の文字を動かさない置換を**長さ r の巡回置換**といって，$(\alpha_1, \alpha_2, \cdots\cdots, \alpha_r)$ で表す．たとえば，$n=6$ のとき，

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 2 & 6 \end{pmatrix} = (2\ 4\ 5)$$

このとき，$(4\ 5\ 2)$ と書いても $(5\ 2\ 4)$ と書いてもよい．$n=6$ をはっきりと示す必要があれば，$(2\ 4\ 5)\ (1)\ (3)\ (6)$ と表す．

とくに，2項の巡回置換 $(\alpha\,\beta)=(\beta\,\alpha)$ を**互換**という．

問 1. 巡回置換 $(1\ 2\ 3\ 4)$ は4乗してはじめて恒等置換となる．すなわち，$(1\ 2\ 3\ 4)$ の位数は4であることを示せ．

一般に長さ r の巡回置換の位数は r である．

問 2. $(1\ 2\ 3\ 4\ 5)^{-1} = (5\ 4\ 3\ 2\ 1)$ を示せ．

任意の置換は互いに共通の文字を含まない巡回置換の積に分解される．積の順序を無視すれば，その分解は一意的である．

たとえば，

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 2 & 6 & 3 & 1 & 7 \end{pmatrix}$$

において，$1 \longmapsto 4 \longmapsto 6 \longmapsto 1$，$2 \longmapsto 5 \longmapsto 3 \longmapsto 2$，$7 \longmapsto 7$ と，それ自身で置き変えられる文字の組を除けば，文字が2組に分けられ，各組で巡回置換 $(1\ 4\ 6)$，$(2\ 5\ 3)$ が引き起こされている．したがって，動かない文字を省くことにすれば，$\sigma=(1\ 4\ 6)\ (2\ 5\ 3)$．

例題 1. 1) 長さ r の巡回置換は $(r-1)$ 個の互換の積に分解される．

2) 任意の置換は互換の積に分解される．

3) 任意の置換は $(1\ k)$, $k=2, \cdots\cdots, n$, の積に分解される.

証明 1) $(\alpha_1\,\alpha_2 \cdots\cdots \alpha_r)=(\alpha_1\alpha_r)\cdots\cdots(\alpha_1\alpha_2)$

2) 任意の置換は巡回置換の積に分解されるから, 1) より明白.

3) $(\alpha\,\beta)=(1\ \alpha)\ (1\ \beta)\ (1\ \alpha)$ であるから, 2) より明白.

例題 2. 任意の置換は $(k, k+1)$, $k=1, 2, \cdots\cdots, n-1$, の形の互換の積に表される.

証明 互換 $(1\ k)=(1\ 2)\ (2\ 3)\ \cdots\cdots(k-1, k)\ \cdots\cdots\ (2\ 3)\ (1\ 2)$ であるから, 上の例題の 3) から出る.

例題 3. n 次対称群 $\mathfrak{S}_n$ は $(1\ 2)$ と $(1\ 2 \cdots\cdots n)$ とで生成される.

証明 $\tau=(1\ 2)\ (1\ 2\ \cdots\cdots\ n)=(2\ 3\ \cdots\cdots\ n)$ であり, $(2\ 3\ \cdots\cdots\ n)\ (1\ 2)\ (2\ 3\ \cdots\cdots\ n)^{-1}=(1\ 3)$, 一般に $\tau^i(1\ 2)\tau^{-i}=(1, 2+i)$, $i\leqq n-2$, である. 例題 1 の 3) から, 任意の置換は $(1\ 2)$ と $(1\ 2\ \cdots\cdots\ n)$ の巾の積になり, したがって, $\mathfrak{S}_n$ は $(1\ 2)$ と $(1\ 2\ \cdots\cdots\ n)$ によって生成される.

さて, 例題 1 に示したように, 任意の置換は互換の積に分解されるが, その分解の仕方は, たとえば, $(1\ 3\ 4\ 2)=(1\ 2)\ (1\ 4)\ (1\ 3)=(1\ 2)\ (1\ 4)\ (1\ 2)\ (2\ 3)\ (1\ 2)$ が示すように一意的でない. しかし, どのように互換の積に分解しても, 現れる互換の数が偶数であるか奇数であるかは, 表し方に無関係に一定であることをつぎに示す.

置換 σ を共通の文字を含まない巡回置換の積 $\sigma_1\sigma_2\cdots\cdots\sigma_t$ に分解したとき, 各 σ_i の長さが r_i として, いま,

$$n(\sigma) = (r_1 - 1) + (r_2 - 1) + \cdots\cdots + (r_t - 1)$$

とおく. ところで,

$$(\alpha\ \beta)(\alpha\ \gamma_1\cdots\cdots\gamma_h\ \beta\ \delta_1\cdots\cdots\delta_k) = (\alpha\ \gamma_1\cdots\cdots\gamma_h)(\beta\ \delta_1\cdots\cdots\delta_k)$$

$$(\alpha\ \beta)(\alpha\ \gamma_1\cdots\cdots\gamma_h)(\beta\ \delta_1\cdots\cdots\delta_k) = (\alpha\ \gamma_1\cdots\cdots\gamma_h\ \beta\ \delta_1\cdots\cdots\delta_k)$$

であるから, 積 $\sigma_1\cdots\cdots\sigma_t$ で, α, β が同じ巡回置換に入っていれば, $n((\alpha\ \beta)\sigma)=n(\sigma)-1$. α, β が異なる巡回置換に入っていれば, $n((\alpha\ \beta)\sigma)=n(\sigma)+1$. いずれにしても $n\ ((\alpha\ \beta)\sigma)=n(\sigma)\pm1$. さて, σ が m 個の互換の積 $(\alpha_1\ \beta_1)\cdots\cdots(\alpha_m\ \beta_m)$ であると, $(\alpha_i\ \beta_i)\ (\alpha_i\ \beta_i)=I$ であるから, $(\alpha_m\ \beta_m)\cdots\cdots(\alpha_1\ \beta_1)\sigma=I$. $n(I)=0$ であるから, $n(\sigma)\pm1\pm1\cdots\cdots\pm1=0$. ここ

で，±1 は m 回現れる．m 個の $+1$ と -1 のうち，$+1$ が m_1 個，-1 が m_2 個とすれば，$n(\sigma)=m_2-m_1$, $m_1+m_2=m$ であるから，$n(\sigma)=m-2m_1$. したがって，σ によって定まる $n(\sigma)$ が偶数となるのは m が偶数のとき，またそのときに限る．

[定義]　偶数個の互換の積に表される置換を**偶置換**，奇数個の互換の積に表される置換を**奇置換**という．

問 3.　長さ r の巡回置換は，r が偶数なら奇置換，r が奇数なら偶置換であることを示せ．

[定理 4]　n 次対称群 $\mathfrak{S}_n$ の偶置換の全体 $\mathfrak{A}_n$ は1つの群をつくる．これを **n 次交代群**という．$\mathfrak{A}_n$ の位数は $n!/2$ である．

[証明]　2つの偶置換の積は偶置換であるから，$\sigma,\ \tau\in\mathfrak{A}_n \Longrightarrow \sigma\tau\in\mathfrak{A}_n$. 恒等置換 $I=(\alpha\ \beta)\ (\alpha\ \beta)$ であるから，$I\in\mathfrak{A}_n$．また，偶置換 $\sigma=(\alpha_1\ \beta_1)\cdots\cdots(\alpha_{2r}\ \beta_{2r})$ の逆 $\sigma^{-1}=(\alpha_{2r}\ \beta_{2r})\cdots\cdots(\alpha_1\ \beta_1)$ であるから，$\sigma^{-1}\in\mathfrak{A}_n$．したがって，$\mathfrak{A}_n$ は1つの群をつくっている．ρ を奇置換とすれば，$\rho\mathfrak{A}_n=\{\rho\sigma|\sigma\in\mathfrak{A}_n\}$ は奇置換ばかりからなる．いま，τ を奇置換とすれば $\rho^{-1}\tau$ は偶置換で，$\rho^{-1}\tau\in\mathfrak{A}_n$, $\tau\in\rho\mathfrak{A}_n$．したがって，$\rho\mathfrak{A}_n$ は奇置換の全体で，$\mathfrak{S}_n$ は偶置換の全体 $\mathfrak{A}_n$ と奇置換の全体 $\rho\mathfrak{A}_n$ とに分けられる．ところで，$\mathfrak{A}_n$ も $\rho\mathfrak{A}_n$ も同じ個数の元からなるので，$\mathfrak{A}_n$ の元の個数は $n!/2$ である．

$\mathfrak{S}_2$ は恒等置換 $e=(1)$ と $(1\ 2)$ からなる巡回群で，$\mathfrak{A}_2$ は e のみからなる．$\mathfrak{S}_3$ は e, $(1\ 2)$, $(1\ 3)$, $(2\ 3)$, $(1\ 2\ 3)$, $(1\ 2\ 3)^2=(1\ 3\ 2)$ からなる位数6の非可換群で，$\mathfrak{A}_3$ は e, $(1\ 2\ 3)$, $(1\ 2\ 3)^2$ からなる位数3の巡回群である．$\mathfrak{S}_4$ は $4!=24$ 個の元からなり，$\mathfrak{A}_4$ は e, $(1\,2\,3)$, $(1\ 2\ 3)^2$, $(1\ 2\ 4)$, $(1\ 2\ 4)^2$, $(1\ 3\ 4)$, $(1\ 3\ 4)^2$, $(2\ 3\ 4)$, $(2\ 3\ 4)^2$, $(1\ 2)\ (3\ 4)$, $(1\ 3)\ (2\ 4)$, $(1\ 4)\ (2\ 3)$ からなる位数12の群である．

例題 4.　n 次交代群 $\mathfrak{A}_n$ はすべての長さ3の巡回置換で生成される．

証明　$(\alpha\ \beta\ \gamma)=(\alpha\ \beta)(\beta\ \gamma)$ であるから，$(\alpha\ \beta\ \gamma)\in\mathfrak{A}_n$. したがって $(\alpha\ \beta\ \gamma)^{-1}\in\mathfrak{A}_n$. 一般に3項巡回置換の積は $\mathfrak{A}_n$ に入る．つぎに，$\sigma=(\alpha\ \beta)(\gamma\ \delta)$ は，2つの互換が同じ互換であれば，$\sigma=I$. また，たとえば，$\beta=\gamma$, $\alpha\neq\delta$ ならば，$\sigma=(\alpha\ \beta\ \delta)$．2つの互

換が共通の文字を含まなければ，$\sigma=(\alpha\ \beta)(\beta\ \gamma)(\beta\ \gamma)(\gamma\ \delta)=(\alpha\ \beta\ \gamma)(\beta\ \gamma\ \delta)$ となる．さて，$\mathfrak{A}_n$ の元は偶数個の互換の積であるから，左または右から順に互換を2つずつくくって考えれば，$\mathfrak{A}_n$ の元は，上に示したことより，3項巡回置換の積となる．

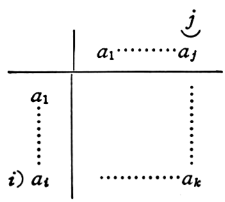
問 4. $\mathfrak{S}_n$ の偶置換は $(1\ k)$, $k=2, \cdots\cdots, n$, の形の互換の偶数個の積として表されることを示せ．このことから，$\mathfrak{A}_n$ は $(1\ i\ j)$ という形の3項巡回置換で生成されることをみちびけ．またここで，$i<j$ と限ってよいことを示せ．

問 5. $(1\ k)\ (1\ 2)=(1\ 2\ k)$, $(1\ 2)\ (1\ k)=(1\ 2\ k)^{-1}$, $(1\ i)\ (1\ k)=(1\ i)(1\ 2)\ (1\ 2)\ (1\ k)=(1\ 2\ i)\ (1\ 2\ k)^{-1}$ を示し，このことから，$\mathfrak{A}_n$ は $n-2$ 個の3項巡回置換 $(1\ 2\ 3), (1\ 2\ 4), \cdots\cdots, (1\ 2\ n)$ から生成されることを示せ．

1-5 同　　型

有限群 G の元を $a_1, a_2, \cdots\cdots, a_n$ とする．いま，$a_ia_j=a_k$ であるとき，i 行 j 列目に a_k をおいた n 行 n 列の元の表を G の**乗積表**という．

表 1-3



たとえば，$\mathfrak{S}_3$ の元 $e, (1\ 2), (1\ 3)(2\ 3), (1\ 2\ 3), (1\ 3\ 2)$ をそれぞれ，e, a, b, c, u, v で表し，乗積表をつくれば，表1-4のようになる．

表 1-4

	e	a	b	c	u	v
e	e	a	b	c	u	v
a	a	e	v	u	c	b
b	b	u	e	v	a	c
c	c	v	u	e	b	a
u	u	b	c	a	v	e
v	v	c	a	b	e	u

乗積表では各行に相異なる元がならび，また各列に相異なる元がならんでいる．またアーベル群の乗積表は，左上から右下にかけての対角線に関して対称になっていることは，表のつくり方から明らかである．

点Oを中心とする正三角形をそれ自身に重ねる回転全体のつくる3次の2面体群 D_3 を考えてみる．正三角形の頂点に1, 2, 3と番号をつけ，図のような対称軸 ZZ', YY', XX' に関する鏡映をそれぞれ a', b', c' とし，Oを通って正三角形に垂直な直線のまわり

の 120° の回転を u', 240° の回転を v' とすれば，D_3 は恒等置換 e', a', b', c', u', v' からなり（p. 19,（6）の（c)），D_3 の乗積表は先の $\mathfrak{S}_3$ の乗積表で，各文字に $'$ をつけたものになる．

それは，D_3 の回転が，頂点 1, 2, 3 の置換を引き起こしているからである．

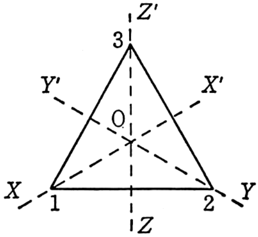


図 1-17

D_3 と $\mathfrak{S}_3$ は抽象的に考えれば同じ群である．このように抽象的には同じとみられる群が具体的にはいろいろな形で表れることがある．

いま，G, G' を 2 つの群として，G から G' への 1 対 1 の写像 φ が，

$$\varphi(xy) = \varphi(x)\varphi(y) \quad \forall x, y \in G$$

をみたすとき，φ を G から G' への**同型**（**同型写像**）という．とくに，φ が G から G' の上への同型であるとき，G と G' は**同型である**といい，記号 $G \cong G'$ で表す．

G から G' への同型 φ があるとき，G の単位元 e には G' の単位元 e' が，G の元 a の逆元 a^{-1} には，a に対応する G の元 a' の逆元 a'^{-1} が対応する．

なぜなら，$\varphi(e)\varphi(e)=\varphi(ee)=\varphi(e)$ であるから，$\varphi(e)$ は G' の単位元であり，また，$\varphi(a)\varphi(a^{-1})=\varphi(aa^{-1})=\varphi(e)=e'$ であるから，$\varphi(a^{-1})=\varphi(a)^{-1}=a'^{-1}$ となる．

$G \cong G'$ で，その同型対応が $a_i \longmapsto a_i'$ であれば，G' の乗積表は G の乗積表で a_i を a_i' で置き変えれば得られるから，G と G' の乗積表は全く同じである．

例 1.　整数の加法群 $\boldsymbol{Z}$ と無限巡回群 $\langle a \rangle$ は，$\varphi(n)=a^n$ により同型である．実際，$\varphi(n+m)=a^{n+m}=a^n a^m=\varphi(n)\varphi(m)$．

問 1.　整数の加法群 $\boldsymbol{Z}$ は偶数全体のつくる加法群と同型であることを示せ．

例題 1.　正 4 面体群 V は 4 次交代群 $\mathfrak{A}_4$ と同型である[1]．

1）巻末文献〔8〕〔10〕〔21〕参照．

証明 正4面体の4頂点を1, 2, 3, 4とすれば，Vの各元は4文字の置換を引き起こす．$V\ni f$に，それが引き起こす置換を対応させれば，Vは$\mathfrak{S}_4$に同型にうつされる．とくに，中心Oと頂点4を通る直線のまわりの回転には$(1\ 2\ 3)$が，Oと頂点3を通る直線のまわりの回転には$(1\ 2\ 4)$が対応している．したがって，同型対応φによるVの像$\varphi(V)$は$\mathfrak{A}_4$を含む（p. 29, 問5参照）．したがって，$\varphi(V)$は少なくとも12個の元を含む．一方，Vの同型像$\varphi(V)$は12個の元からなるから，$\varphi(V)=\mathfrak{A}_4$である．

例題 2． 正6面体群は$\mathfrak{S}_4$と同型である[1]．

証明 正6面体群Gは，(1) 向かい合った2辺の中点を結ぶ直線のまわりの回転と，(2) 向かい合った頂点を結ぶ直線$a=$A′A, $b=$B′B, $c=$C′C, $d=$D′Dをそれぞれ軸とする回転と，(3) 向かい合った面の中心を結ぶ直線のまわりの回転とからなる．$G\ni f$はa, b, c, dの置換を引き起こす．これを$\varphi(f)$で表す．CBの中点MとC′B′の中点M′を結ぶ直線のまわりの回転で，

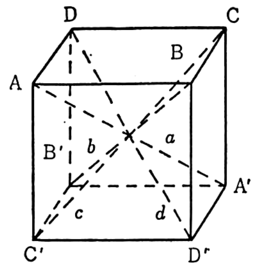


図 1-18

AとA′，DとD′が入れ変わり，aはaに，dはdに重なる．一方，BとC，B′とC′が入れ変わるので，bとcは入れ変わる．したがって，$\varphi(f)=(b\ c)$．

つぎに，正方形ABCDの中心Nと，正方形A′B′C′D′の中心N′を結ぶ．N′からNに向かう向きを正とする直線N′Nのまわりの90°の回転gによって，a, b, c, dは巡回的に入れ変わるから，$\varphi(g)=(a\ b\ c\ d)=(b\ c\ d\ a)$．したがって，$\varphi(G)$は$(b\ c)$，$(b\ c\ d\ a)$を含むので，p. 27の例題3によって，$\varphi(G)=\mathfrak{S}_4$となる．$G$も$\mathfrak{S}_4$も24個の元からなるから，$\varphi$は1対1の対応で，$G$と$\mathfrak{S}_4$は同型である．

注 正20面体群は5次交代群と同型である．巻末文献〔8〕,〔10〕〔21〕参照．

問 題 1

1． $G=\{(a, b)|a, b$は実数，$a\neq 0\}$において，$(a, b)(c, d)=(ac, bc+d)$とすれば，Gは群となる．

1） 巻末文献〔8〕〔10〕〔21〕参照．

2.　変換 $\varphi_{a,b}(x)=ax+b$ $(a,\ b\in\boldsymbol{R},\ a\neq 0)$ の全体は群をつくる.

3.　$E=\{a|a\in\boldsymbol{R},\ |a|<1\}$ として, E の任意の元 $a,\ b$ について $a\circ b=(a+b)/(1+ab)$ とすれば, E は群をつくる.

4.　集合 $\{e,\ (1\ 2)\ (3\ 4),\ (1\ 3)\ (2\ 4),\ (1\ 4)\ (2\ 3)\}$ は, クラインの4元群と同型な群をつくる.

5.　巡回置換 $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ で生成された巡回群のすべての元をあげよ.

6.　4次の対称群 $\mathfrak{S}_4$ は $(1\ 2)$ と $(2\ 3\ 4)$ で生成される.

7.　6次の2面体群 D_6 の各回転は, 6個の文字 1, 2, 3, 4, 5, 6 の置換を引き起こす. D_6 と同型な, 6個の文字の置換のつくる群を求めよ.

8.　集合 $\{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$ で, $i^2=j^2=k^2=-1,\ ij=-ji=k,\ jk=-kj=i,\ ki=-ik=j$ とすれば, この集合は位数8の非可換群をつくる (この群を**4元数群**という).

9.　1)　$u=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ v=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ で生成された群は D_4 と同型である.

2)　$x=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ y=\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix},\ \xi=e^{2\pi i/n}$ とすれば, $x,\ y$ が生成する群は D_n と同型である.

2

部　分　群

2-1 部　分　群

2-1-1 部　分　群

整数全体 $\boldsymbol{Z}$ は加法に関して群をつくり，偶数全体は同じく加法に関して群をつくっている．また，3 次対称群 $\mathfrak{S}_3$ の中で，偶置換の全体は 3 次交代群 $\mathfrak{A}_3$ をつくっている．このように，群 G の部分集合 H が G と同じ演算に関して群をつくるとき，H を G の**部分群**という．部分群 H の単位元を e', G の単位元を e とすれば，$e'e'=e'=ee'$ であるから，$e'=e$ となり，H の単位元と G の単位元は一致する．また，部分群 $H\ni a$ の H における逆元を a' とすれば，$a'a=e$ であるから，$a'=a^{-1}$．すなわち，H の元 a の逆元は H で考えても G で考えても一致する．今後，H が群 G の部分群であることを $G>H$，または，$H<G$ で表す．

［定理 1］　群 G の部分集合 H が部分群であるための必要十分条件は，

(1)　$a, b\in H \Longrightarrow ab\in H$

(2)　$a\in H \Longrightarrow a^{-1}\in H$

が成り立つことである．

［証明］　$H<G$ であれば，定義と上に述べたことから，(1), (2) が成り立つ．つぎに十分であることを示す．$H\subset G$ であるから，H では結合法則は成り立つ．(2) より逆元の存在がいえ，さらに $H\ni a$ に対して $a^{-1}\in H$ であるから，(1) より $aa^{-1}=e\in H$, すなわちHの中に単位元が存在する．したがって，H は群をつくる．

例題 1.　群 G の部分集合 H が部分群であるための必要十分条件は，

(3)　$H\ni a, b \Longrightarrow ab^{-1}\in H$

が成り立つことである．

証明　$H<G$ ならば，$H\ni a, b$ に対して，(2) より $b^{-1}\in H$ であるから，(1) より $ab^{-1}\in H$ となる．逆に (3) が成り立てば，$H\ni a$ に対して (3) の a と b が一致する場合として，$e=aa^{-1}\in H$，したがって $ea^{-1}=a^{-1}\in H$ となって (2) が成り立つ．$H\ni a, b$ のとき，$b^{-1}\in H$ であるから，$ab=a(b^{-1})^{-1}\in H$ となり，(1) が成り立つ．したがって，H は部分群である．

群 G の 2 つの部分集合 S, T に対して，

$$ST=\{st|s\in S, t\in T\},\qquad S^{-1}=\{s^{-1}|s\in S\}$$

と定義する．とくに，S が唯一つの元 s からなるときは ST を sT と書く．一般には $ST\neq TS$．定義からただちにつぎの等式がみちびかれる．

$$(S^{-1})^{-1}=S,\qquad (ST)R=S(TR),\qquad (ST)^{-1}=T^{-1}S^{-1}$$

群 G 自身に対しては，つぎの等式が成り立つ．

$$G^{-1}=G,\qquad GG=G,\qquad aG=Ga=G\quad \forall a\in G$$

実際 G の各元 x に対して，$x^{-1}\in G$ であるから，$x=(x^{-1})^{-1}\in G^{-1}$ となり，$G\subset G^{-1}$，したがって $G=G^{-1}$．また $e\in G$ であるから，$GG\supset Ge=G$，したがって $GG=G$．さらに G の任意の元 x に対して $a^{-1}x\in G$ であって，$x=a(a^{-1}x)\in aG$ となるから $G\subset aG$，したがって，$aG=G$．同様にして $Ga=G$ がいえる．

この記号を使えば，定理 1 や例題 1 はつぎのようにいってよい．

$$G>H \Leftrightarrow (1')\quad HH\subset H \qquad (2')\quad H^{-1}\subset H$$

$$G>H \Leftrightarrow (3')\quad HH^{-1}\subset H$$

加法群 G においては，その部分集合 H が部分群であるための必要十分条件は，

(1″)　$a, b\in H \Longrightarrow a+b\in H$　　(2″)　$a\in H \Longrightarrow -a\in H$

あるいは，

(3″)　$a, b\in H \Longrightarrow a-b\in H$

例 1.　0 でない実数全体のつくる乗法群 $\boldsymbol{R}^*$ の中で，0 でない有理数の全体 $\boldsymbol{Q}^*$ は部分群である．

例 2.　整数全体のつくる加法群 $\boldsymbol{Z}$ の中で，偶数全体 $2\boldsymbol{Z}$ は部分群である．

群 G の単位元 e はこれだけで部分群をつくる．これを G の**単位群**という．G 自身も G の部分群である．G の部分群 H は $\{e\}\subsetneqq H\subsetneqq G$ であるとき，G の**真の部分群**という．

例題 2． 群 G の部分集合 H が有限集合のとき，

$$G>H \Leftrightarrow (☆)\quad a,\ b\in H \text{ であれば，} ab\in H$$

証明 （☆）が成り立つとする．H の任意の元 a に対し，a の正巾はすべて H に含まれるが，H が有限集合ゆえ，$a^h=a^k(h>k>0)$ となる $h,\ k$ が存在する．したがって $a^{h-k}=e,\ h-k>0$．いま，n を $a^n=e$ となる最小自然数とすれば，$a^{-1}=a^{n-1}\in H$ となり，定理 1 により $H<G$ となる．$G>H$ ならば，（☆）が成り立つことは明白．

注 H が有限集合でないと成り立たないことがある．$\boldsymbol{R}^*$ の中で奇数全体を H とすると，（☆）が成り立つが，H は群をつくっていない．

例題 3． $G>H,\ G>K \Longrightarrow G>H\cap K$

証明 $a,\ b\in H\cap K$ ならば，$a,\ b\in H$ ゆえ，$ab^{-1}\in H$．同様に $ab^{-1}\in K$ であるから，$ab^{-1}\in H\cap K$ となる．したがって，$H\cap K<G$．

［定理 2］ $G>H,\ G>K$ のとき，

$$G>HK \Leftrightarrow HK=KH$$

［証明］ $HK=KH$ が成り立てば，$(HK)(HK)^{-1}=HKK^{-1}H^{-1}=HKH=HHK=HK$ であるから，$HK<G$．
逆に，$HK<G$ であれば，$HK=(HK)^{-1}=K^{-1}H^{-1}=KH$

2-1-2 巡 回 部 分 群

M を群 G の部分集合とするとき，M に属する有限個の元 $a_{r_1},\ \cdots\cdots,\ a_{r_n}$ の巾積 $a_{r_1}^{e_1}\cdots\cdots a_{r_n}^{e_n}$ の全体は 1 つの部分群をつくる．これを，**M から生成された部分群**といって，$\langle M\rangle$ で表す．たとえば，5 次の 2 面体群 D_5 は p. 23, (8) で述べたように，$\sigma^5=\tau^2=e,\ \sigma\tau=\tau\sigma^4$ をみたす $\sigma,\ \tau$ で生成されているので，$D_5=\langle\sigma,\ \tau\rangle$．

いま，群 G の元 a に対して，$H=\{a^m,\ m=0,\ \pm1,\ \pm2,\ \cdots\cdots\}$ は G の部分群である．実際，$H\ni a^m,\ a^n$ ならば，$a^m(a^n)^{-1}=a^{m-n}\in H$ である．この部分群 H を **a で生成された巡回部分群**といい，$H=\langle a\rangle$ で表す．このとき，a

を H の**生成元**という．とくに，$G=\langle a\rangle$ のとき，p. 25，(9) で述べたように，G を **a で生成された巡回群**という．

加法群 G においては，a で生成された巡回部分群 $\langle a\rangle=\{ma|m=0,\pm 1,\pm 2,\cdots\cdots\}$ である．

群 G の元 a によって生成された $\langle a\rangle$ が位数 n の有限群のとき，n を元 a の**位数**という．$\langle a\rangle$ が無限群のとき，元 a の位数は無限大であるという．元 a の位数を $o(a)$ で表すことがある．

p. 25，(9) で述べたように，

［定理 3］　巡回群 $G=\langle a\rangle$ において，

(1)　$a^m=e$ をみたす自然数 m が存在すれば，G は有限巡回群である．このような m のうち最小の自然数を n とすれば，G の，したがって a の位数は n であって，G は n 個の元 $a^0=e, a, a^2, \cdots\cdots, a^{n-1}$ からなる．また，$a^k=e$ となるのは，k が n の倍数のとき，そのときに限る．

(2)　G が無限巡回群ならば，$\cdots\cdots, a^{-2}, a^{-1}, a^0=e, a, a^2, \cdots\cdots$ はすべて互いに異なる．

例題 1．　a, b が位数 m, n の元で，$ab=ba$ であれば，ab の位数は m, n の最小公倍数の約数である．もしも m と n が互いに素であれば，ab の位数はちょうど mn である．

証明　m, n の最小公約数を l とすると，$(ab)^l=a^lb^l=e$ であるから，$o(ab)$ は l の約数である．また，$(m, n)=1$ のときは $l=mn$ である．いま，$(ab)^r=e$ とすれば $a^rb^r=e$, $a^r=b^{-r}$, $e=b^{-rn}=a^{rn}$. よって，$m|rn$ となり $m|r$. 同様にして，$n|r$. $(m, n)=1$ ゆえ，$mn|r$, $l|r$. したがって，$l|o(ab)$ であるから，先の結果と合せて $o(ab)=l=mn$.

問 1．　有限群 G の 2 つの元 a, b に対し $o(ab)=o(ba)$.
（$o(ab)=s$ とするとき，$e=(ab)^s=abab\cdots\cdots ab=a(ba)\cdots\cdots(ba)b=a(ba)^{s-1}b$ であることを使え）

［定理 4］　巡回群 $G=\langle a\rangle$ が無限巡回群ならば，G の生成元は a と a^{-1} の 2 つだけである．G が位数 n の有限巡回群であれば，a の 巾 a^r が G の生成元であるための必要十分条件は r と n が互いに素であることである．

［証明］ $\langle a\rangle=\langle b\rangle$ とすると，$b=a^r$, $a=b^s$ となるから，

$$a=b^s=a^{rs},\ a^{rs-1}=e.$$

G が無限巡回群のときは $rs-1=0$, $rs=1$. よって，$r=\pm 1$ となるから，$b=a$ または $b=a^{-1}$ である．

G が位数 n の有限巡回群のときは $rs-1=nt$, $rs-nt=1$ となるから，r と n は互いに素である．逆に r と n が互いに素ならば，$b=a^r$ とおくとき，$b^m=a^{rm}=e$ とすれば，$n|rm$, $n|m$. 一方，$b^n=a^{rn}=e$ であるから，b の位数は n で，$\langle b\rangle$ は n 個の元 $b^0=e, b, \cdots\cdots, b^{n-1}$ を含むので，$\langle b\rangle\subset\langle a\rangle$ より，個数を比べて $\langle b\rangle=\langle a\rangle$ となる．

位数 n の巡回群 $\langle a\rangle$ の生成元は全部で，a^r, $1\leqq r\leqq n-1$, r, n は互いに素である，であって，その個数は，1, 2, ……, n のうち n と互いに素であるものの個数 $\varphi(n)$ に等しい．この自然数に対して定義される関数 φ を**オイラー**(Euler)**の関数**という．

［定理 5］ 巡回群 $G=\langle a\rangle$ の部分群はすべて巡回群である．G が位数 n の有限巡回群であれば，その部分群の位数は n の約数である．また，n の任意の約数 m を位数とする部分群が1つ，唯一つ存在する．

［証明］ $H\neq\{e\}$ を G と異なる部分群とすると，$a^i\in H$, $i\neq 0$ となる a^i がある．$i<0$ であれば，$a^{-i}\in H$, $-i>0$ であるから，H の中には a^j, $j>0$ という元がある．かかる j のうち最小の自然数を h とすれば，$H=\langle a^h\rangle$ となる．なぜならば，H の元 a^k に対し，$k=hq+r$, $0\leqq r<h$ とおくとき，$a^k, a^{hq}\in H$ より，$a^r=a^ka^{-hq}\in H$ となり，h の最小性より $r=0$, よって $h|k$ となる．

G が無限群であれば，$\langle a^h\rangle$, $h=0, 1, 2, \cdots\cdots$ によって，G のすべての部分群が得られる．

G が位数 n の有限群ならば，$a^n=e\in H$ であるから，$n=hm$ となり，$H=\langle a^h\rangle$ は m 個の元 $a^0=e, a^h, a^{2h}, \cdots\cdots, a^{(m-1)h}$ からなる．

逆に，m が n の約数なら，$n=mh$ とすれば，$H_m=\langle a^h\rangle$ は位数 m の巡回部分群となる．したがって，G の部分群は $H_m=\langle a^h\rangle$，ここで，$h=n/m$ でつくされる．

問 2. 位数 24 の巡回群 $\langle a\rangle$ の部分群をすべて求め，それらの包含関係を示せ．

問 3. 群 $G\neq\{e\}$ が真の部分群をもたなければ，G は巡回群で，その位数は素数である（まず G が有限巡回群であることを示せ）．

問 4. 無限巡回群 $G=\langle a\rangle$ の極大部分群は $\langle a^p\rangle$ である．ここで，p は素数である．群 G の真の部分群 H は，$G>K>H$ ならば，必ず $K=G$ か $K=H$ と

なるときに，**極大部分群**という．

例題 2. 巡回群 $G=\langle a\rangle$ の位数を n とし，m を n の約数とすれば，$x^m=e$ となる G の元 x 全体は位数 m の部分群をつくる．

証明 $x=a^k$ とすれば，$a^{km}=e$ より $n=mh$ は mk の約数，$h|k$ となるから，$k=hl$，$x=a^{hl}\in\langle a^h\rangle=H_m$．逆に，$H_m$ の元 y は $y^m=e$ をみたす．したがって，$H_m=\langle a^h\rangle=\{x|x\in G,\ x^m=e\}$．

例題 3. 巡回群 $G=\langle a\rangle$ の位数が n ならば，部分群 $\langle a^k\rangle$ の位数 n' は n/k' である．ここで $k'=(n,k)$，n と k の最大公約数である．

証明 $(a^k)^{n'}=a^{n'k}=e$ より $n|n'k$．したがって，n/k' は $n'(k/k')$ の約数であり，n' は n/k' で割り切れる．一方，$(a^k)^{n/k'}=(a^n)^{k/k'}=e$ であるから，n/k' は n' で割り切れる．したがって，$n'=n/k'$．

定理5の応用として，つぎの整数の最大公約数の性質を証明してみよう．

例題 4. 整数 $a_1, a_2, \cdots\cdots, a_n$ の最大公約数を d とすると，

$$a_1b_1+a_2b_2+\cdots\cdots+a_nb_n=d$$

となる整数 $b_1, b_2, \cdots\cdots, b_n$ が存在する．

証明 整数全体のつくる加法群 $\boldsymbol{Z}$ は，1を生成元とする無限巡回群である．$H=\{a_1x_1+\cdots\cdots+a_nx_n,\ 各\ x_i\in\boldsymbol{Z}\}$ は $\boldsymbol{Z}$ の部分群である．実際，$a_1x_1+\cdots\cdots+a_nx_n$，$a_1y_1+\cdots\cdots+a_ny_n\in H$ なら，

$$(a_1x_1+\cdots\cdots+a_nx_n)-(a_1y_1+\cdots\cdots+a_ny_n)$$
$$=a_1(x_1-y_1)+\cdots\cdots+a_n(x_n-y_n)\in H$$

となる．さて，H は巡回群で，$H=\langle d\rangle$，H は d の倍数全体である．各 $a_i\in H$ であるから，a_i は d の倍数で，d は $a_1, \cdots\cdots, a_n$ の公約数である．一方，$d\in H$ であるから，

$$d=a_1b_1+\cdots\cdots+a_nb_n,\qquad 各\ b_i\in\boldsymbol{Z}$$

と表されるので，$a_1, a_2, \cdots\cdots, a_n$ の公約数は d の約数である．したがって，d は $a_1, a_2, \cdots\cdots, a_n$ の最大公約数である．

この例題の特別な場合として，つぎのよく使われる事柄が得られる．

整数 a, b が互いに素である $\Leftrightarrow$ 整数 x, y により $ax+by=1$

例題 5. 群 G の元 a の位数が mn で，$(m,n)=1$ であれば，a は位数が m の元 b と位数が n の元 c との可換の積に，一意的に表される．

証明　$(m, n)=1$ であるから，$mh+nk=1$ となる整数 h, k が存在する．$b=a^{nk}$, $c=a^{mh}$ とおけば $a=bc=cb$ となる．a^n の位数は m で，$(m, k)=1$ であるから，$b=a^{nk}$ の位数も m であり，同様に $c=a^{mh}$ の位数は n である．つぎに，$a=b'c'=c'b'$, b' の位数は m, c' の位数は n とすると，$a^{nk}=b'^{nk}c'^{nk}=b'^{nk}=b'^{mh+nk}=b'$ であるから，$b'=b$. したがって，$a=bc=bc'$ より $c'=c$ となる．

問 5.　p が有限群 G の位数の素因数であれば，G の元 a は，位数が p の巾である元 a_p と，位数が p と素である元 b_p との可換な積に，一意的に表される．

問 6.　$G=\langle a\rangle$ を無限巡回群とする．$G_1=\langle a^m\rangle$, $G_2=\langle a^n\rangle$ とし，m, n の最大公約数を g とすれば，$\langle a^g\rangle$ は G_1 の元と G_2 の元の積の全体である．

例題 6.　有限群 G が巡回群であるための必要十分条件は，任意の自然数 n に対して，$x^n=e$ となる G の元 x の個数が n 以下であることである．

特別な場合として，0 以外の複素数のつくる乗法群 $\boldsymbol{C}^*$ の有限部分群 H は巡回群である．

証明　条件が必要なこと．　G が位数 g の巡回群ならば，$x^g=e$. $x^n=e$ であり，$(g, n)=d=gh+nk$, h, k は整数，となるから，$x^d=e$. このような x は，例題 2 に示したように d 個あり，$d\leqq n$.

条件が十分なこと．　G の位数を g とし，G は条件をみたすとする．いま，別に，C を位数 g の巡回群とする．G の任意の元 a の位数を m とすると，巡回群 $\langle a\rangle$ の m 個の元 $e, a, \cdots\cdots, a^{m-1}$ は $x^m=e$ をみたし，仮定によって，G の中には $x^m=e$ の解はたかだか m 個しかないから，これら m 個の元が $x^m=e$ の解すべてになる．したがって，G において位数 m の元はすべて $\langle a\rangle$ に含まれ，それは $\langle a\rangle$ の生成元であるから，その個数は $\varphi(m)$ である．一方，巡回群 C において，$m|g$ であるから，$x^m=e$ をみたす元 x の全体は，例題 2 で示したように，位数 m の部分群 H_m をつくり，C において，位数 m の元は，H_m の生成元であるから，その個数は $\varphi(m)$ である．さて，G の元を位数によって分類し，位数が $m_1=1, m_2, \cdots\cdots, m_r$ の元がそれぞれ $\varphi(m_1)=1, \varphi(m_2), \cdots\cdots, \varphi(m_r)$ だけあって，これで G の元がつくされるとすれば，C においても，位数が $m_1, m_2, \cdots\cdots, m_r$ の元がそれぞれ G の場合と同数だけあって，それらの合計が g である．したがって，C の中には位数 g の元があることから，$g=1+\cdots\cdots+\varphi(g)$ となっているので，G の中にも位数 g の元 u が存在し，よって $G=\langle u\rangle$. (証明中の $m|g$ については p. 43, 定理 8 を見よ.)

問 7.　実数のつくる有限乗法群は $\{1, -1\}$ だけである．

2-1-3 類別・剰余類

集合 M を互いに共通元を含まない，空でない部分集合 $A, B, C,$ ……に分けることを M を**類別する**といい，各部分集合を**類**という．M は類 $A, B, C,$ ……の和集合で，これを $M=A+B+C+\cdots\cdots$ で表すことがある．

1つの類 A から任意にとった元 a を A の**代表元**といい，類 $A, B, C,$ ……のおのおのから1つずつ代表元 $a, b, c,$ ……をとってできる集合 $\{a, b, c, \cdots\cdots\}$ を，この類別の**完全代表系**という．

たとえば，整数の集合 $\boldsymbol{Z}$ を偶数の全体と奇数の全体に分けることは1つの類別である．このとき，同じ類に含まれる a, b に対して $a-b$ は2で割り切れ，c, d が異なる類に属すれば $c-d$ は2で割れない．いま，整数 a, b は $a-b$ が2で割り切れるとき，2を法として合同であるといって，記号 $a\equiv b \pmod 2$ で表すことにすれば，つぎの3条件がみたされる．

(1) **反射律**　$a\equiv a \pmod 2$

(2) **対称律**　$a\equiv b \pmod 2 \Longrightarrow b\equiv a \pmod 2$

(3) **推移律**　$a\equiv b,\ b\equiv c \pmod 2 \Longrightarrow a\equiv c \pmod 2$

$a-a=0$ は2で割り切れるから $a\equiv a$. $a-b$ が2で割り切れれば，$b-a$ も2で割り切れるから，(2) が成り立つ．$a-b, b-c$ がともに2で割り切れれば，$a-c=(a-b)+(b-c)$ も2で割り切れるから，(3) も成り立つ．

一般に，ある集合 M の元の間に1つの関係 $a\equiv b$ が定義されていて，この関係が上記の3つの条件をみたすとき，この関係は**同値律**をみたす，または**同値関係**であるという．そうして $a\equiv b$ であるとき，a と b は**同値**であるという．場合によっては合同，相似，同型等といわれ，また記号 $\equiv$ のほかに $\sim$ などが用いられることがある．a と b が同値でないことを $a\not\equiv b$ で表す．

集合 M の元の間に同値関係が定義されているとき，a と同値な M の元すべての集合を**同値類**といい，C_a で表す：$C_a=\{x | x\in M,\ a\equiv x\}$．反射律によって，$a\in C_a$. また $C_a\cap C_b\neq\phi$ ならば $C_a=C_b$ である．それは，$C_a\cap C_b\ni c$ とすれば，$a\equiv c,\ b\equiv c$. $x\in C_b$ ならば $b\equiv x$. 反射律によって $x\equiv b$. $x\equiv b,\ b\equiv c$ より推移律によって $x\equiv c$. $a\equiv c$ より反射律によって $c\equiv a$. $x\equiv c,\ c\equiv a$

より推移律によって $x \equiv a$. ゆえに $x \in C_a$, $C_b \subset C_a$. 同様にして $C_a \subset C_b$ がいえて, $C_a = C_b$. 対偶をとれば, $C_a \neq C_b$ ならば $C_a \cap C_b = \phi$.

以上によって, M の異なる同値類を全部集めれば, M の任意の元はある同値類に属し, 異なる同値類は共通元を含まないから, M の1つの類別が得られる. 1つの同値類に属する元は互いに同値であり, 異なる同値類に属する元は同値でない. 実際, $C_a \ni b, c$ ならば $a \equiv b$, $a \equiv c$ より $b \equiv c$ となり, 逆に $b \equiv c$ ならば $b, c \in C_c$ であるから, b, c は同じ同値類に入る.

逆に, 集合 M が類別されているとき, M の2つの元 a, b が同じ類に属するとき $a \equiv b$ とすれば, この関係は同値律をみたし, この同値関係による類別ははじめの類別と一致している.

例 1. m を1つの定まった整数として, $a-b$ が m で割り切れるとき, a と b は m を法として合同であるといい, $a \equiv b \pmod{m}$ で表す. この同値関係によって整数全体は m 個の同値類に分けられる.

さて, 群の類別について考えよう. H を群 G の部分群とする. G の元 a, b は $b = ah$ となる H の元 h が存在するとき, H を法として**右合同**であるといい, $a \equiv b \pmod{H}_r$ で表す. $ae = a$. $b = ah$, $h \in H$, ならば, $bh^{-1} = a$ で $h^{-1} \in H$. また, $ah = b$, $bh' = c$, $h, h' \in H$, ならば $ahh' = c$ で, $hh' \in H$ である. したがって, この関係は同値律をみたす. よって, G は類別されて, 元 a を含む同値類は,

$$x \equiv a \pmod{H}_r \Leftrightarrow x = ah,\ h \in H \Leftrightarrow x \in aH$$

であるから, $aH = \{ah \mid h \in H\}$ である. $h \in H$ のとき $hH = H$ であるから, H は1つの同値類で, これは単位元 e を含む同値類である. 同値類 aH を H を法とする**右剰余類**という. G は異なる右剰余類の和として,

$$G = a_1H + a_2H + \cdots\cdots$$

と類別される. これを G の H による**右分解**という.

H による G の右分解では $a \equiv b \pmod{H}_r$ をつぎのように表せる.

1) $\exists h \in H$, $b = ah$ ($b = ah$ となるような H の元 h が存在する)

2) $b \in aH$

3) $a^{-1}b \in H$

4) $aH = bH$

つぎに，$b=ha$ となる H の元 h が存在するとき，a と b は H を法として**左合同**であるといい，$a \equiv b \pmod{H}_l$ で表す．この関係も同値律をみたし，各同値類は Ha という形をしていることは，右合同の場合と同様にしてわかる．類 Ha を H を法とする**左剰余類**という．

注 本によっては左合同，右合同の言葉の使い方が逆の場合がある．

群 G がアーベル群のときは，$ah=ha$ であるから，左合同と右合同は同じことになり，単に**合同**という．また，このとき部分群による類別では左剰余類と右剰余類の区別はなくなり，単に**剰余類**といい，a と b が部分群 H を法として合同であることを $a \equiv b \pmod{H}$ で表す．

例 2. 整数の加法群 $\boldsymbol{Z}=\langle 1\rangle$ を巡回部分群 $\langle m\rangle$ を法として剰余類に分けることは，先の例1に述べた類別にほかならない．今後，

$$a \equiv b \pmod{\langle m\rangle}$$

のことを簡単に，

$$a \equiv b \pmod{m}$$

と書く．

例題 1. 群 G の部分群 H による右分解を，

$$G = a_1H + a_2H + \cdots\cdots$$

とすれば，つぎの分解は，G の H による左分解である．

$$G = Ha_1^{-1} + Ha_2^{-1} + \cdots\cdots$$

証明 x を G の任意の元として，$x^{-1} \in a_iH$ とすれば，$x \in (a_iH)^{-1} = H^{-1}a_i^{-1} = Ha_i^{-1}$ となり，G の任意の元はある左剰余類 Ha_i^{-1} に入る．つぎに，$Ha_i^{-1} = Ha_j^{-1}$ とすれば $Ha_j^{-1}a_i = H$, $a_j^{-1}a_i \in H$, $a_i \in a_jH$. したがって $a_iH = a_jH$, $i=j$ となるから，Ha_1^{-1}, Ha_2^{-1}, ……はすべて互いに異なる．したがって，G の左分解 $G = Ha_1^{-1} + Ha_2^{-1} + \cdots\cdots$ を得る．

この例題から，H を法とした右，左剰余類の間に1対1の対応 $a_iH \longleftrightarrow Ha_i^{-1}$ がつくから，右，左の剰余類の個数は，無限個のときは1対1の

対応がつくという意味で，等しい．この個数を H の G における**指数**といって $|G:H|$ または $(G:H)$ で表す．とくに，$H=\{e\}$ のときは，その指数 $|G:\{e\}|$ は G の位数 $|G|$ にほかならない．

問 1． 群 G の部分群 H を法とした異なる右剰余類から1つずつとった代表元の全体を H に関する**右代表系**という．$\{a_1, a_2, \cdots\cdots\}$ が右代表系であれば，G の任意元 a に対して，$\{aa_1, aa_2, \cdots\cdots\}$ も右代表系である．

例題 2． H, K は群 G の部分群で，$G>H>K$ とする．指数 $|G:H|$, $|H:K|$ がともに有限であれば，

$$|G:K| = |G:H||H:K|$$

証明 $G=a_1H+\cdots\cdots+a_rH$, $H=b_1K+\cdots\cdots+b_sK$ とする．G の任意元 $a=a_ih=a_ib_jk$, $H\ni h=b_jk$, $k\in K$, と表されるから，$aK=a_ib_jK$. つぎに $a_ib_jK=a_kb_lK$ とすれば，$a_ib_j=a_kb_lk$, $k\in K$ より $a_i\in a_kH$. よって $a_i=a_k$, さらに $b_j=b_l$ となる．ゆえに，G の K を法とする右剰余類は a_ib_jK, $i=1, 2, \cdots\cdots, r$, $j=1, 2, \cdots\cdots, s$ で与えられるので，$|G:K|=|G:H||H:K|$.

特に G を有限群とし，H を G の部分群，K を単位群とすれば，

$$|G| = |G:H||H|$$

となるから，つぎの定理が得られる．

[定理 6] 有限群の位数は，その部分群の位数と指数の積に等しい．

[定理 7] **(ラグランジュ)**

有限群 G の部分群の位数ならびに指数は G の位数の約数である．

特別な場合として，

[定理 8] 有限群の各元の位数は群の位数 n の約数である．したがって，任意の元 a について，$a^n=e$ が成り立つ．

[証明] 元 a の生成する巡回部分群 $\langle a\rangle$ に定理7を適用すればよい．

問 2． 位数が素数の群は巡回群であり，真の部分群をもたない．

例題 3． 3次対称群 $\mathfrak{S}_3$ の部分群をすべて求めよ．

解 $\mathfrak{S}_3$ の位数は6であるから，真の部分群は位数は2か3かである．

位数2の部分群：位数2の置換ごとに1つずつつくられる．

$$H_1 = \{e, (1\ 2)\},\ H_2 = \{e, (1\ 3)\},\ H_3 = \{e, (2\ 3)\}$$

位数 3 の部分群は 3 次交代群 $\mathfrak{A}_3=\{e, (1\ 2\ 3), (1\ 3\ 2)\}=\langle(1\ 2\ 3)\rangle$ 1 つだけである.

4 次の対称群 $\mathfrak{S}_4$ の真の部分群は, $|\mathfrak{S}_4|=24$ であるから, その位数は 2, 3, 4, 6, 12 のいずれかである. すべての部分群をあげるのはそう簡単ではないので, もう少し群の一般的な性質がわかってからにする (p. 106, 例題 6). 4 次交代群 $\mathfrak{A}_4$ の位数は 12 で, 12 の真の約数は 2, 3, 4, 6 である. $\mathfrak{A}_4$ は位数 2, 3 および 4 の部分群としてそれぞれ $\langle(1\ 2)\ (3\ 4)\rangle$, $\langle(1\ 2\ 3)\rangle$ および $\{e, (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}$ をもつが, 位数 6 の部分群をもたない (p. 61).

例題 4. 位数 4 の群は, 巡回群か, クラインの 4 元群の 2 つだけである.

証明 G を位数 4 の群とする. G が位数 4 の元 a を含めば, $G=\langle a\rangle$. G が位数 4 の元を含まないときは, G の単位元以外の元は位数は 2 である. したがって, G の各元 x について $x^2=e$, $x=x^{-1}$ となるから,

$$xy=(xy)^{-1}=y^{-1}x^{-1}=yx$$

となって, G はアーベル群である. いま, $G=\{e, a, b, c\}$ とする. $ab=e$ なら $a=b^{-1}=b$ となり, $ab=a$ なら $b=e$ となり, $ab=b$ なら $a=e$ となるから, $ab=ba=c$. さらに $bc=cb=abb=a$, $ca=ac=aab=b$ であるから, G はクラインの 4 元群である (p. 20, 例 6 (d)).

つぎに正 8 面体群 V の類別を考えてみよう. 正 8 面体の 6 個の頂点に図 2-1 のように記号をつける. V に属する回転で A_1 を動かさないものは軸 A_1A_6 のまわりの 4 個の回転で, これらは位数 4 の巡回部分群 H をつくる. A_1 を A_i にうつす回転を σ_i とすれば, σ_iH に属する回転はすべて A_1 を A_i にうつす. 逆に, A_1 を A_i にうつす回転 τ は σ_iH に属す. なぜなら, $\sigma_i^{-1}\tau$ は A_1 を動かさない回転で, $\sigma_i^{-1}\tau\in H$

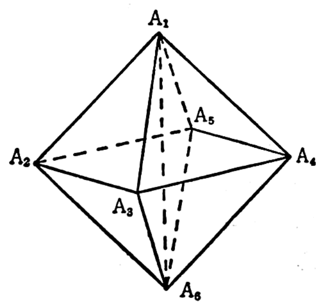


図 2-1

となるから．V に属する回転は，A_1 をどれかの頂点にうつすから，σ_1H, σ_2H, σ_3H, σ_4H, σ_5H, σ_6H のいずれかに属する．$i \neq j$ であれば，$\sigma_iH \cap \sigma_jH = \phi$ であるから，$V=\sigma_1H+\sigma_2H+\cdots\cdots+\sigma_6H$ である．各類 σ_iH は $|H|=4$ 個の元を含むから，$|V|=4\cdot 6=24$.

正多面体群 G の位数 N は，上のようにして，1つの頂点を動かさない回転すべてがつくる部分群 H による右分解によって求められる．正多面体の頂点の個数を v，1つの頂点に集まる辺の個数を p_1 とすれば，$|H|=p_1$ で，$|G:H|=v$ であるから，$N=|G|=p_1v$ である．

正4面体，正6面体，正8面体，正12面体，正20面体の順に p_1v の値をあげれば，$3\times4=12$, $3\times8=24$, $4\times6=24$, $3\times20=60$, $5\times12=60$ となる（p. 23，表1-2）．

H, K は群 G の2つの部分群とする．G の2つの元 a, b は，

$$b = hak, \quad h\in H,\ k\in K$$

であるとき，同値であると定義すると，この関係は同値律をみたしている．したがって，G は類別され，a の属する類は HaK である．この類別を H, K による G の**両側分解**といい，その各類を H, K を法とした**両側剰余類**という．HaK は集合として H を法とした左剰余類 Hak, $k\in K$, の和集合であり，また K を法とした右剰余類 haK, $h\in H$, の和集合である．

とくに，$H=K$ のとき，類 HaH を **Hを法とした両側剰余類**という．

さて，H を群 G の部分群とするとき，$G\ni a$ に対して $a^{-1}Ha$ も G の部分群である．なぜなら，$H\ni h, h'$ とすれば，$(a^{-1}ha)(a^{-1}h'a)^{-1}=a^{-1}haa^{-1}h'^{-1}a=a^{-1}hh'^{-1}a\in a^{-1}Ha$ であるから．

[定理 9]　H, K を群 G の部分群とする．HaK に含まれる左剰余類 Hak, $k\in K$, の個数は（無限個のときは，1対1の対応がつくという意味で）K の $K\cap a^{-1}Ha$ を法とした左剰余類の個数 $|K: K\cap a^{-1}Ha|$ に等しい．また HaK に含まれる右剰余類 haK, $h\in H$, の個数は H の $H\cap aKa^{-1}$ を法

とした右剰余類の個数 $|H:H\cap aKa^{-1}|$ に等しい.

［証明］　$Hak_1=Hak_2,\ k_1,\ k_2\in K \Leftrightarrow ak_1k_2^{-1}a^{-1}\in H \Leftrightarrow k_1k_2^{-1}\in K\cap a^{-1}Ha \Leftrightarrow k_1\in(K\cap a^{-1}Ha)k_2$ であるから, HaK に含まれる左剰余類と $K\cap a^{-1}Ha$ を法とした左剰余類との間に1対1対応 $Hak \longleftrightarrow (K\cap a^{-1}Ha)k$ がつく. 後半も同様にして証明される.

［系 1］　H, K を群 G の部分群とする. HK に含まれる K を法とした右剰余類の個数は H の $H\cap K$ を法とした右剰余類の個数に等しい.

とくに, HK が部分群であれば,

$$|HK:K|=|H:H\cap K|,\qquad |HK:H|=|K:H\cap K|$$

［系 2］　H, K を群 G の部分群とする. $|G:H|$ が有限であれば,

$$|K:H\cap K|\leqq|G:H|$$

問 3.　H は群 G の部分群, N は G の, $NH=HN$ であるような部分群で, H の指数が有限であれば, $|N:N\cap H|$ は $|G:H|$ の約数である.

［定理 10］　H, K を群 G の部分群とする. $|G:H|, |G:K|$ がともに有限であれば, $|G:H\cap K|\leqq|G:H||G:K|$ である. ここで, 等号が成り立つのは $G=HK$ のとき, そのときに限る.

［証明］　$|G:H\cap K|=|G:H||H:H\cap K|\leqq|G:H||G:K|$

後半を示す. $G=HK$ であれば, 定理9系1より, $|G:K|=|H:H\cap K|$ であって, 等号が成り立つ. 逆に等号が成り立てば, $|G:K|=|H:H\cap K|$ で, 集合 HK に含まれる K を法とした右剰余類は $|H:H\cap K|=|G:K|$ 個あるから $HK=G$.

［系］　$H_1, H_2, \cdots\cdots, H_r$ は G の指数が有限な部分群とすれば, これら部分群の共通集合も指数有限な部分群である.

問 4.　H, K は群 G の部分群で, $|G:H|$ と $|G:K|$ がともに有限で, 互いに素であれば, $G=HK$.

2-2 正規部分群・剰余群

2-2-1 正規部分群

群 G の部分集合 S について，

$$tSt^{-1} = \{tst^{-1} | s \in S\}, \quad t \in G$$

を S を t で変換した部分集合，または S に**共役な**部分集合という．とくに，G の部分群 H に共役な tHt^{-1} はまた G の部分群である．実際，$h_1, h_2 \in H$ のとき，$(th_1t^{-1})(th_2t^{-1})^{-1} = th_1h_2^{-1}t^{-1} \in tHt^{-1}$ であるから，tHt^{-1} は G の部分群である．tHt^{-1} を H に**共役な部分群**，または，H の**共役部分群**という．

[定義]　群 G の部分群 N に共役な部分群が N だけしかないとき，すなわち，

$$tNt^{-1} = N \quad \forall t \in G$$

であるとき，N を G の**正規**（または不変）**部分群**という．N が G の正規部分群であることを記号 $G \triangleright N$ または $N \triangleleft G$ で表す．

注　幾分弱く，$tNt^{-1} \subset N$, $\forall t \in G$ のとき，N を G の正規部分群といってもよい．実際，t の代りに t^{-1} をとれば，$t^{-1}Nt \subset N$，ゆえに，$t(t^{-1}Nt)t^{-1} = N \subset tNt^{-1}$ となり，結局，$tNt^{-1} = N$ となる．

問 1.　群 G の部分群 H と共役な部分群 $H' = tHt^{-1}$ は，対応 $x \longmapsto txt^{-1}$ によって同型である．また，対応 $aH \longmapsto (tat^{-1})H'$ によって，G の H を法とする右剰余類と，H' を法とする右剰余類は1対1に対応する．したがって，$|G:H| = |G:H'|$

群 G は G 自身と単位群 $\{e\}$ を自明な正規部分群としてもつ．これら以外に正規部分群をもたない群を**単純群**という．たとえば，位数が素数の群は単純である．また，アーベル群の部分群はすべて正規部分群である．

問 2.　アーベル群が単純群ならば，位数が素数の巡回群である．

例題 1.　群 G の指数が2の部分群は正規部分群である．

証明　H を G の指数2の部分群とする．$a \in G$, $a \notin H$ のとき $aH \neq H$, $Ha \neq H$ で，$|G:H| = 2$ ゆえ，$G = H + aH = H + Ha$．ゆえに，$Ha = aH$．$a \in H$ のときは $H = Ha$

$=aH$. ∴ $Ha=aH \quad \forall a \in G$.

例 1. 交代群 $\mathfrak{A}_n$ は対称群 $\mathfrak{S}_n$ の正規部分群である.

なぜなら，σ を奇置換とすれば，$\sigma\mathfrak{A}_n$ は奇置換の全体で，$\mathfrak{S}_n=\mathfrak{A}_n+\sigma\mathfrak{A}_n$ となり，$|\mathfrak{S}_n:\mathfrak{A}_n|=2$ であるから.

例 2. H, K が群 G の正規部分群ならば，$H\cap K$ も G の正規部分群である. 実際，$\forall a\in G$, $aH=Ha$, $aK=Ka$ であるから，$a(H\cap K)=aH\cap aK=Ha\cap Ka=(H\cap K)a$ となる. ∴ $H\cap K \lhd G$.

問 3. $G \rhd H$, $G>K \Longrightarrow H\cap K \lhd K$.

例題 2. H, K は群 G の部分群で，どちらか一方，たとえば K が正規部分群であれば，HK は G の部分群である. H, K ともに正規部分群であれば，HK は G の正規部分群である.

$HK=HH^{-1}KH=KH$

証明 p. 35，定理2から $HK=KH$ をいえばよい. 実際に，$HK=\bigcup hK$, h は H 全体を動く，$=\bigcup Kh=KH$. 後半をいう. $\forall a\in G$, $aHKa^{-1}=(aHa^{-1})\ (aKa^{-1})=HK$ であるから，$HK \lhd G$.

[定義] 群 G の部分集合 M の各元と可換な G の元の集合

$$\{x|x\in G,\ xc=cx\ \ \forall c\in M\}$$

は G の部分群をつくる. これを M の**中心化群**といい，$Z_G(M)$ または $Z(M)$ で表す.

実際，$x, y\in Z(M)$ ならば，$xc=cx$, $yc=cy\ \ \forall c\in M$ で，$xyc=xcy=cxy$ ゆえ，$xy\in Z(M)$. また，$xc=cx$ より $x^{-1}c=cx^{-1}$ であるから，$x^{-1}\in Z(M)$. ゆえに $Z(M)<G$.

[定義] とくに，群 G の中心化群 $Z(G)$ を G の**中心**または**核心**という. G の中心を Z_G，または Z で表すことがある.

$$\text{中心}\quad Z=\{x|x\in G,\ xc=cx\quad \forall c\in G\}$$

G の中心 Z に属する元は互いに可換であるから，Z はアーベル群である. また，Z は G の正規部分群であり，Z に含まれる部分群は G の正規部分群である.

[定義] M が群 G の部分集合のとき，$xM=Mx$ である G の元 x の

集合

$$\{x|x\in G,\ xM=Mx,\ \text{つまり}\ xMx^{-1}=M\}$$

は G の部分群をつくる．これを M の**正規化群**といい，$N_G(M)$，または $N(M)$ で表す．

実際，$x,\ y\in N(M)$ とすれば，$xMx^{-1}=yMy^{-1}=M$ であるから，$xyM(xy)^{-1}=xyMy^{-1}x^{-1}=xMx^{-1}=M$ $\therefore$ $xy\in M$．また，$xMx^{-1}=M$ より $x^{-1}Mx=M$ $\therefore$ $x^{-1}\in M$．したがって，$N(M)<G$．

集合 M が唯一の元 a からなる場合，$Z(M)$, $N(M)$ をそれぞれ $Z(a)$, $N(a)$ と書く．この場合，$Z(a)=N(a)$ である．

定義から明らかなように $Z(M)\subset N(M)$ である．また，H が G の部分群であれば，$H<N(H)$ である．

問 4. $Z(aMa^{-1})=aZ(M)a^{-1}$, $N(aMa^{-1})=aN(M)a^{-1}$ を示せ．

例題 3. 群 G の部分群 H の正規化群 $N(H)$ は，H を正規部分群として含む G の最大の部分群である：$G>G'$, $G'\triangleright H \Longrightarrow G'\subset N(H)$.

証明 $H\ni x$ なら $xHx^{-1}=H$ であるから，$H<N(H)$ である．つぎに，$G>G'$, $G'\triangleright H$ とすれば，G' の任意元 x について $xHx^{-1}=H$ であるから，$x\in N(H)$．
$\therefore$ $G'\subset N(H)$.

［定理 11］ 群 G の部分集合 M の共役集合と，G の $N(M)$ を法とする右剰余類の間に1対1の対応がつく．したがって，M の共役集合の個数は $|G:N(M)|$ に等しい．

［証明］ $aMa^{-1}=bMb^{-1} \Leftrightarrow a^{-1}bMb^{-1}a=M \Leftrightarrow a^{-1}b\in N(M) \Leftrightarrow b\in aN(M)$ であるから，$G=a_1N(M)+a_2N(M)+\cdots\cdots$ を G の $N(M)$ による右分解とすれば，$a_1Ma_1^{-1}$, $a_2Ma_2^{-1}$, $\cdots\cdots$ はすべて互いに異なり，M の共役集合はこれでつくされる．$a_iN(M)\longleftrightarrow a_iMa_i^{-1}$ が求める1対1対応である．

［系］ 群 G の部分群 H の共役群の個数は，指数 $|G:H|$ より大きくない．とくに有限指数の部分群の共役群の個数は有限である．

2-2-2 剰　余　群

群 G の正規部分群 N による類別では，G の任意の元 a に対し $aN=Na$ であるから，右剰余類と左剰余類は一致し，これを単に**剰余類**とよんでよい．また，左合同と右合同の区別がないので，単に**合同**とよぶ．

N を法とする剰余類の全体 $\bar{G}=\{Na|a\in G\}$ は，Na と Nb の積を $NaNb=Nab$ と定義すれば，1つの群をつくる．この結合は類の代表のとり方に無関係である．なぜならば，$Na=Na'$, $Nb=Nb'$ とすれば，$a'=h_1a$, $b'=h_2b$ で，$a'b'=h_1ah_2b=h_1h_2'ab$，ここで，h_1, h_2, $h_2'\in N$ であるから，$Nab=Na'b'$．明らかに結合法則は成り立つ．$Ne=N$ は，$NNa=Na$ より，左単位元であり，Na に対して Na^{-1} は，$Na^{-1}Na=Na^{-1}a=Ne=N$ であるから，左逆元である．したがって，$\bar{G}$ は群となり，N が単位元，Na の逆元 $(Na)^{-1}=Na^{-1}$ である．

［定義］　N を群 G の正規部分群とするとき，N を法とする G の剰余類全体は乗法群をつくる．これを N を法とする G の **剰余(類)群** といい，G/N で表す．剰余群は**因子群**または**商群**ともよばれる．

剰余群 G/N の位数は指数 $|G:N|$ に等しい．G/N において，Na を $\bar{a}$ で表せば，乗法の定義から $\bar{a}\bar{b}=\overline{ab}$.

例 1.　G の G を法とする剰余群 G/G は単位元 G のみからなり，G の単位群 $\{e\}=E$ を法とする剰余群 G/E は G にほかならない．

例 2.　アーベル群の剰余群はすべてアーベル群である．

例 3.　$G=\langle a\rangle$ を巡回群，N をその部分群とすれば，G/N は，$A=Na$ とおくとき，A から生成された巡回群である．

$$G=\langle a\rangle,\quad G/N=\langle A\rangle,\quad A=Na$$

$N\neq\{e\}$ であれば，m を $a^m\in N$ となる最小自然数とするとき，$N=\langle a^m\rangle$ であって，G/N の，したがって A の位数は m である．

例題 1.　N を群 G の中心に含まれる部分群，したがって正規部分群，とする．G/N が巡回群であれば，G はアーベル群である．

証明　$G/N=\langle Na\rangle$ であるから，$G=\bigcup Na^i$．$Z\supset N$ であるから，G の任意の元 ha^i,

$h'a^j$，ここで，$h, h' \in N$，に対して $ha^ih'a^j = hh'a^ia^j = h'ha^ja^i = h'a^jha^i$ である．したがって，G はアーベル群である．

例題 2. N は有限群 G の正規部分群で，N の位数 n と指数 m が互いに素であれば，$N = \{x | x \in G,\ x^n = e\} = \{y^m | y \in G\}$ である．

証明 $(n, m) = 1$ であるから，$rn + sm = 1$ となる整数 s, t が存在する．$x^n = e$ ならば，$x = x^{nr}\, x^{ms} = x^{ms}$．ところが，$G/N$ の位数は m であるから，$(xN)^m = x^m N = N$，$x^m \in N$．ゆえに，$x \in N$．逆に，$x \in N$ であれば，明らかに $x^n = e$．これで，上のはじめの等式が示された．つぎに，x を N の任意の元とすれば，$x^n = e$ ゆえ，上に示したように，$x = x^{ms} = (x^s)^m$．逆に，$y \in G$ であれば，G/N の位数が m であるから，$y^m \in N$．これで第二式も示された．

2-2-3 既約剰余類群

整数全体 $\boldsymbol{Z}$ を正の整数 m を法として類別すれば，m 個の同値類に分けられる（p. 41，例 1）．$\boldsymbol{Z} \ni a$ の属する同値類を C_a で表すと，$a = mq + r$，$0 \leqq r < m$ となる整数 q, r が存在するから，$a \equiv r \pmod{m}$ で，a は $C_0, C_1, \cdots\cdots, C_{m-1}$ のどれかに入り，C_a はこれら m 個の類のどれかと一致する．ところで $\boldsymbol{Z}$ は加法群として無限巡回群 $\langle 1 \rangle$ であり，$N = \langle m \rangle$ とすると，N を法とする $\boldsymbol{Z}$ の剰余類は m を法とする同値類にほかならない：$a \equiv b \pmod{\langle m \rangle} \Leftrightarrow a \equiv b \pmod{m}$．剰余群 $\boldsymbol{Z}/N$ は加法が $C_a + C_b = C_{a+b}$ で定義されている加法群で，C_0 が零元，C_a の逆元（マイナス元）$-C_a = C_{-a}$ で，$\boldsymbol{Z}/N$ は C_1 を生成元とする位数 m の巡回群である．

ところで，つぎの合同式が成り立つ．

$$a \equiv a', \quad b \equiv b' \pmod{m} \Longrightarrow ab \equiv a'b' \pmod{m}$$

なぜなら，$ab - a'b' = a(b - b') + (a - a')b'$ であり，$b - b'$，$a - a'$ は m で割り切れるから，$ab - a'b'$ は m の倍数．

したがって，$C_a = C_{a'}$，$C_b = C_{b'}$ ならば $C_{ab} = C_{a'b'}$ である．そこで，m 個の剰余類の集合 $\boldsymbol{Z}_m = \{C_0, C_1, \cdots\cdots, C_{m-1}\}$ において，乗法を $C_a C_b = C_{ab}$ と定義しよう．$C_a C_b = C_{ab} = C_{ba} = C_b C_a$ であるから，交換法則が成り立ち，$(C_a C_b) C_c = C_{ab} C_c = C_{abc} = C_a C_{bc} = C_a (C_b C_c)$ であるから，結合法則も成り立

つ．$C_1C_a=C_aC_1=C_a$ であるから，C_1 は単位元である．しかし，たとえば，$m=6$ のとき，$C_3 \neq C_0$, $C_4 \neq C_0$ にもかかわらず，$C_3C_4=C_{12}=C_0$ となり，$2n \not\equiv 1$ であるから，$C_2C_n=C_1$ となる C_n は存在しない．このように $\boldsymbol{Z}_m$ 全体も，$\boldsymbol{Z}_m$ から零元 C_0 を除いた残りも必ずしも乗法群というわけでない．いま，$\boldsymbol{Z}_m$ の中で m と互いに素であるような a の属する C_a だけに着目してみる．$a+mt$ も m と互いに素であるから，C_a の数はすべて m と素である．このような m と互いに素である整数からなる剰余類を**既約剰余類**という．既約剰余類は逆元をもつ．すなわち，a が m と互いに素であれば，$ax+my=1$ となる整数 x, y が存在するから，$ax\equiv 1 \pmod{m}$, したがって，$C_aC_x=C_1$ となる．逆に C_a が逆元 C_x をもてば，$ax\equiv 1 \pmod{m}$ であるから，$ax+my=1$ となる整数 x, y が存在するから，a と m は互いに素であって，C_a は既約剰余類である．

［定義］　m を正の整数とするとき，m を法とする既約剰余類の全体は乗法に関してアーベル群をつくり，その位数は $\varphi(m)$ である．この群を m を法とする（または法 m の）既約剰余類群といい，$\boldsymbol{Z}_m{}^*$ で表す[1]．

例 1.　8を法とする既約剰余類群は，4つの類 C_1, C_3, C_5, C_7 からなる．たとえば，$C_3C_5=C_7$. $C_3C_3=C_1$ ゆえ，$C_3{}^{-1}=C_3$.

例題 1.　**（オイラーの定理）**　m を正の整数，a を m と互いに素な整数とすると，

$$a^{\varphi(m)}\equiv 1 \pmod{m}$$

証明　$\boldsymbol{Z}_m{}^*$ の位数は $\varphi(m)$ であるから，$a\in C_a$ に対して $C_a{}^{\varphi(m)}=(C_a)^{\varphi(m)}=C_1$. したがって，$a^{\varphi(m)}\equiv 1 \pmod{m}$ となる．

例 2.　p を素数とすると，C_0 を除く $p-1$ 個の剰余類 $C_1, C_2, \cdots\cdots, C_{p-1}$ が既約剰余類で，これらは乗法群をつくる．したがって，

$$a^{p-1}\equiv 1 \pmod{p} \quad \forall a,\ p\nmid a \quad (p \text{ は } a \text{ を割らない})$$

注　この事実を**フェルマー** (Fermar) の定理という．

問 1.　整数 a が素数 p で割り切れないとき，$a^f\equiv 1 \pmod{p}$ となる最小自然数

1）付録2参照．

f は $p-1$ の約数である．

注 素数 p に対して，$p-1$ 乗してはじめて1と合同になる整数の存在がわかっている[1]．このような整数 a は合同式 $x^{p-1}\equiv 1 \pmod p$ の根で，$1\leqq h<p-1$ である h に対しては $a^h\equiv 1 \pmod p$ とはならないから，p を法とする1の**原始根**とよばれる．たとえば，$p=5$ に対し，$a\equiv 2 \pmod 5$ である a は原始根である．法 p の既約剰余類群 $\boldsymbol{Z}_p{}^*$ は位数が $p-1$ の巡回群で，a を原始根とすれば，C_a が生成元である．たとえば，$p=5$ のとき，$C_2{}^2=C_4$, $C_2{}^3=C_2C_4=C_3$, $C_2{}^4=C_2C_3=C_1$ で，$\boldsymbol{Z}_5{}^*=\langle\bar{2}\rangle$．ここで $\bar{2}=C_2$.

［定理 12］ p を素数とする．p の巾 p^m を法とする既約剰余類群 $\boldsymbol{Z}_{p^m}{}^*$ の位数は $\varphi(p^m)=p^{m-1}(p-1)$ である．とくに，$p\neq 2$ であれば，$\boldsymbol{Z}_{p^m}{}^*$ は巡回群である．

［証明］ 1, 2, ……, p^m のうちで，p の倍数は $p, 2p, \cdots\cdots, p^{m-1}p$ の p^{m-1} 個あるから，p と素なものの個数は，

$$\varphi(p^m)=p^m-p^{m-1}=p^{m-1}(p-1)$$

つぎに，$p\neq 2$ とする．p を法として位数 $p-1$ の整数を a とすれば，

$$(a^{p^{m-1}})^{p-1}\equiv 1 \pmod{p^m}$$

いま，$(a^{p^{m-1}})^r\equiv 1 \pmod{p^m}$ とすれば，rp^{m-1} は $p-1$ の倍数であるから，r は $p-1$ の倍数である．ゆえに，p^m を法として，$a^{p^{m-1}}$ の位数は $p-1$ である．一方，帰納法によって，$(1+p)^{p^i}\equiv 1+p^{i+1} \pmod{p^{i+2}}$ が成り立つことがわかる．とくに，$(1+p)^{p^{m-2}}\equiv 1+p^{m-1}\not\equiv 1$, $(1+p)^{p^{m-1}}\equiv 1 \pmod{p^m}$ であるから，p^m を法として，$(1+p)$ の位数は p^{m-1} である．$(p^{m-1}, p-1)=1$ であるから，p^m を法とする $a(1+p)$ の位数は $p^{m-1}(p-1)$ である（p. 36, 例題1）．したがって，$\boldsymbol{Z}_{p^m}{}^*$ は $a(1+p)$ の属する剰余類で生成された巡回群である．

注 p が奇素数のとき，ω の属する法 p^m の剰余類が $\boldsymbol{Z}_{p^m}{}^*$ の生成元となるとき，$\omega \pmod{p^m}$ を **p^m を法とする1の原始根**[2] という．

注 $\boldsymbol{Z}_2{}^*=$単位群，$\boldsymbol{Z}_{2^2}{}^*=\{\bar{1}, \bar{3}\}=\langle\bar{3}\rangle$ である．$m\geqq 3$ のときは，$\boldsymbol{Z}_{2^m}{}^*$ は位数 2^{m-1} の群であるが，もはや巡回群ではない（p. 80 例題5）.

たとえば，$m=4$ のとき $\boldsymbol{Z}_{2^4}{}^*=\{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{15}\}$ は位数4の元 $\bar{5}$ と，位数2の元 $\overline{-1}=\overline{15}$ とから生成されている．実際に，$5^2\equiv 9$, $5^3\equiv 9\cdot 5\equiv 13$,

1) 巻末文献〔23〕,〔24〕,〔25〕参照.
2) 巻末文献〔23〕,〔24〕,〔25〕参照.

$5^4 \equiv 5 \cdot 13 \equiv 1 \pmod{16}$, $15 \cdot 5 \equiv 11$, $15 \cdot 9 \equiv 7$, $15 \cdot 13 \equiv 3 \pmod{16}$.

このとき，$\overline{15}$の代りに$\overline{7}$をとってもよい．

$$7 \cdot 5 \equiv 3, \quad 7 \cdot 9 \equiv 15, \quad 7 \cdot 13 \equiv 11 \pmod{16}$$

2-3 共　役

2-3-1 共　役　類

群 G の元 a に対して，tat^{-1}, $t \in G$ を a を t で変換した元，または a に共役な元という．いま，G の元 b が a に共役なとき，つまり $b=tat^{-1}$ となる $t \in G$ が存在するとき，$a \sim b$ と書くことにする．共役な関係は同値関係である．すなわち，

$$eae^{-1} = a, \quad b = tat^{-1} \Longrightarrow a = t^{-1}bt = (t^{-1})b(t^{-1})^{-1}$$

$$b = tat^{-1}, \ c = sbs^{-1} \Longrightarrow c = (st)a(st)^{-1}$$

問 1.　$a \sim b$ ならば，a の位数と b の位数は等しい．

問 2.　$a \sim b$ ならば $a^2 \sim b^2$, 一般に $a^n \sim b^n$ である．

例 1.

$$\sigma = \begin{pmatrix} 1 & 2 \cdots\cdots & n \\ p_1 & p_2 \ \cdots\cdots & p_n \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & \cdots\cdots & n \\ \tau(1) & \tau(2) & \cdots\cdots & \tau(n) \end{pmatrix}$$

とすると，

$$\tau\sigma\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \cdots\cdots & \tau(n) \\ \tau(p_1) & \tau(p_2) & \cdots\cdots & \tau(p_n) \end{pmatrix}$$

すなわち，$\tau\sigma\tau^{-1}$ は σ の上，下の文字，すなわち，すべての文字を τ による像で置き変えれば得られる．実際，$\tau(i) \overset{\tau^{-1}}{\longmapsto} i \overset{\sigma}{\longmapsto} p_i \overset{\tau}{\longmapsto} \tau(p_i)$ となるからである．たとえば，

$$\sigma = (1\ 2\ 3\ 4), \quad \tau = (2\ 4) \text{ のとき,} \quad \tau\sigma\tau^{-1} = (1\ 4\ 3\ 2)$$

例 2.　σ は定点 O のまわりの回転で，その回転軸を l，回転角を θ とする．τ も O のまわりの回転とすれば，$\tau\sigma\tau^{-1}$ は O のまわりの回転で，その回転軸は τl，回転角は θ である．

まず，l 上の点 $\mathrm{C} \neq \mathrm{O}$ に対し，$\sigma\mathrm{C}=\mathrm{C}$ であるから，$\tau\sigma\tau^{-1}(\tau\mathrm{C})=\tau\sigma\mathrm{C}=\tau\mathrm{C}$. したがって，$\tau l$ 上の点 $\tau\mathrm{C}$ は $\tau\sigma\tau^{-1}$ で不変で，$\tau\sigma\tau^{-1}$ は O と $\tau\mathrm{C}$ を通る直線 τl を

回転軸にもつ．つぎに，任意の点 $A \notin l$ から l に下した垂線の足をCとし，$\sigma A = B$ とすれば，線分 CA を l のまわりに θ だけ回転すれば，CB に重なる．A, B, C の τ による像を A′, B′, C′ とすれば，$A' \overset{\tau^{-1}}{\longmapsto} A \overset{\sigma}{\longmapsto} B \overset{\tau}{\longmapsto} B'$.

さて，$\angle ACB = \theta$ で，τ は合同変換であるから，$\triangle A'B'C'$ は $\triangle ABC$ に合同であり，τl に垂直である．よって，C′A′ を τl のまわりに θ だけ回転すれば C′B′ に重なる．すなわち，$\tau\sigma\tau^{-1}$ の回転角は θ である．

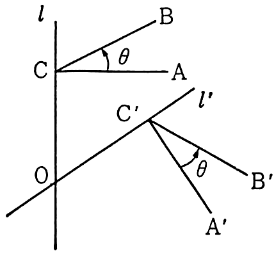


図 2-2

注　回転角は回転軸に向きをつけることによって定まる（p. 6 注）．

いま，回転 τ が σ の回転軸 l の向きを逆にするだけであれば，$\tau\sigma\tau^{-1}$ は，l を軸とする回転角 $-\theta$ の回転であるから，σ の逆回転 σ^{-1} である．

［定義］　共役な関係は同値関係であるから，群 G は類別される．各類は互いに共役な元の集合であって，これを**共役類**という．

元 a が G の中心に属していれば，a の共役は a だけで，a 1つだけで共役類をつくっている．a が中心に属さなければ，a を含む共役類は2つ以上の元を含んでいる．

例 3.　群 G の正規部分群 N はいくつかの，無限個かもしれない，共役類の和集合である．実際 $N \ni a$ に対し，$tat^{-1} \in N$ であるから，a の共役類の元はすべて N に属し，その共役類は N に含まれる．したがって，N はその元 a の共役類の和集合である．

例題 1.　4次の2面体群 D_4 を共役類に分けよ．

解　D_4 は正方形の中心 O のまわりの，正方形をそれ自身に重ねる回転の全体である．D_4 に属する回転を t で変換したものは，回転角は同じで，回転軸を t でうつしたものが回転軸になっている．まず，恒等変換 e はそれだけで1つの共役類をつくる．つぎに，正方形ののっている平面上の，中心 O のまわりの 90° の回転 σ の回

転軸 l は，O を通り，この平面に垂直であるから，l は D_4 の回転で全く動かないか，または向きが逆になる．したがって，σ に共役なものは σ か σ^{-1} $(=\sigma^3$, l のまわりの 270° の回転）である．つぎに，1つの対角線を軸とする 180° の回転を τ とする．この軸は D_4 の回転で全く動かないか，向きが逆になるか，またはもう1つの対角線にうつるかであるから，τ の共役は τ か，もう1つの対角線のまわりの 180° の回転である．後の回転は $\tau\sigma^2$ である．つぎに，$\tau\sigma$ は1対の向かい合う辺の中点を結ぶ直線 g のまわりの 180° の回転で，g は D_4 の回転で全く動かないか，向きが逆になるか，もう1対の向かい合う辺の中点を結ぶ直線 h にうつるかであるから，$\tau\sigma$ の共役は $\tau\sigma$ と，h のまわりの 180° の回転 $\tau\sigma^3$ である．最後に $\sigma\sim\sigma$, $\sigma\sim\sigma^3$ より $\sigma^2\sim\sigma^2$, $\sigma^2\sim\sigma^6=\sigma^2$ であるから，σ^2 は1つだけで共役類をつくる．以上から，D_4 は $\{e\}$, $\{\sigma^2\}$, $\{\sigma, \sigma^3\}$, $\{\tau, \tau\sigma^2\}$, $\{\tau\sigma, \tau\sigma^3\}$ の5つの共役類に分かれる．

問 3.　D_4 の中心は $\{e, \sigma^2\}=\langle\sigma^2\rangle$ である．

2-3-2 類　公　式

[定理 13]　群 G の元 a の共役元と，a の中心化群 $Z(a)$ による G の右剰余類との間に1対1の対応 $tat^{-1} \longleftrightarrow tZ(a)$ がつく．

したがって，a の共役元の個数は指数 $|G:Z(a)|$ に等しい．

[証明]　$tat^{-1}=sas^{-1} \Leftrightarrow t^{-1}sa(t^{-1}s)^{-1}=a \Leftrightarrow t^{-1}sa=at^{-1}s \Leftrightarrow t^{-1}s\in Z(a) \Leftrightarrow s\in tZ(a)$ であるから，G の $Z(a)$ による右分解を $G=t_1Z(a)+t_2Z(a)+\cdots\cdots$ とすれば，$t_1at_1^{-1}$, $t_2at_2^{-1}$, ……はすべて異なり，a の共役元はこれらでつくされ，$t_iat_i^{-1} \longleftrightarrow t_iZ(a)$ が a の共役元と $Z(a)$ を法とした右剰余類との間の1対1対応である．

いま，G を位数 n の有限群とし，G の共役類を $C_1=\{e\}$, C_2, ……, C_k とする．C_i に属する元を a_i とすれば，C_i は a_i に共役な元の全体であるから，C_i に属する元の個数 h_i は $|G:Z(a_i)|$ に等しい．したがって，h_i は n の約数であって，つぎの**類公式**が成り立つ．

$$(*)\qquad n=1+h_2+\cdots\cdots+h_k \quad (h_1=1)$$

とくに，$h_i=1$ となるのは a_i が G の中心 Z に属するとき，そのときに限るから，類公式で，$h_1=h_2=\cdots\cdots=h_z=1$, $i>z$ ならば $h_i>1$ であるように共役類に番号をつければ，$Z=\{a_1=e, a_2, \cdots\cdots, a_z\}$ となり，(*) はつぎのように表される．

(**)　$n = z + h_{z+1} + \cdots\cdots + h_k \quad (z = |Z|,\ h_i > 1)$

[定理 14]　位数が素数の巾の群の中心 Z は単位元 e 以外の元を含む.

[証明]　類公式 (**) において, n も各 h_i も p で割り切れるから, z も p で割り切れる. したがって, $1<z$ であり, Z は e 以外の元を含む.

例題 1.　位数が素数 p の平方の群 G はアーベル群である.

証明　G の中心 Z は単位元 e 以外の元を含む. その1つを a とする. a が G を生成すれば, G はアーベル群である. $G \neq \langle a \rangle$ ならば, 部分群 $A = \langle a \rangle$ は, $a \in Z$ ゆえ, G の正規部分群で, その位数は p である. 剰余群 G/A は位数が素数 p であるから, 巡回群で, $G/A = \langle bA \rangle$ とすれば, $G = A + bA + \cdots\cdots + b^{p-1}A$. G は a と b とで生成され, a は b と可換であるから, G はアーベル群である.

2-3-3　対称群・交代群の共役類

n 次対称群 $\mathfrak{S}_n$ の元 σ を, τ で変換した $\tau\sigma\tau^{-1}$ は, σ の文字をすべて τ によって置き変えれば得られる (p. 54, 例 1).

いま, σ が,

$$\sigma = (a_1 \cdots\cdots a_r)(b_1 \cdots\cdots b_s)\cdots\cdots(k_1 \cdots\cdots k_u),$$

ここで, $r \leqq s \leqq \cdots\cdots \leqq u$, と共通の文字を含まない巡回置換の積 (簡単に, 独立な巡回置換の標準積という) に表されているとき, $\tau\sigma\tau^{-1}$ は,

$$\tau\sigma\tau^{-1} = (\tau(a_1)\cdots\cdots\tau(a_r))(\tau(b_1)\cdots\cdots\tau(b_s))\cdots\cdots(\tau(k_1)\cdots\cdots\tau(k_u))$$

となるから, 整数 $r, s, \cdots\cdots, u$ の組を σ の型ということにすれば, σ と $\tau\sigma\tau^{-1}$ は同じ型である. 逆に σ' が σ と同じ型とすると,

$$\sigma' = (a_1' \cdots\cdots a_r')(b_1' \cdots\cdots b_s')\cdots\cdots(k_1' \cdots\cdots k_u')$$

を σ' の独立な巡回置換の標準積とすれば,

$$\tau = \begin{pmatrix} a_1 \cdots\cdots a_r & b_1 \cdots\cdots b_s \cdots\cdots & k_1 \cdots\cdots k_u \\ a_1' \cdots\cdots a_r' & b_1' \cdots\cdots b_s' \cdots\cdots & k_1' \cdots\cdots k_u' \end{pmatrix}$$

とするとき, $\sigma' = \tau\sigma\tau^{-1}$ となる. 以上まとめて,

[定理 15]　n 次対称群 $\mathfrak{S}_n$ において, 2つの置換 σ, σ' が共役であるための必要十分条件は, それらを独立な巡回置換の標準積に表したとき, 同じ

型をもつことである．したがって，$\mathfrak{S}_n$ の共役類の個数 $p(n)$ は，

$$x_1 + x_2 + \cdots\cdots + x_i = n \quad かつ \quad 0 < x_1 \leqq x_2 \leqq \cdots\cdots \leqq x_i$$

の整数解の，$i=1, 2, \cdots\cdots, n$ についての総和に等しい．

問 1. $p(2)=2$, $p(3)=3$, $p(4)=5$, $p(5)=7$ を確かめよ．

$\mathfrak{S}_n$ の元 σ を独立な巡回置換の標準積に表すとき，k 項の巡回置換の個数を m_k $(k=1, 2, \cdots\cdots, n)$ とすれば，$n=m_1+2m_2+\cdots\cdots+nm_n$ であって，σ の属する共役類は数の組 $(m_1, m_2, \cdots\cdots, m_n)$ によって定まる．そこで $(m_1, m_2, \cdots\cdots, m_n)$ を σ の，また σ の属する共役類のタイプということにする．いま，たとえば $\sigma=(1\ 2\ 3)$ は $(1\ 2\ 3)=(2\ 3\ 1)=(3\ 1\ 2)$ と見掛け上３通りの表し方があり，$\rho=(1\ 2\ 3)(4\ 5\ 6)$ は $\rho_1=(1\ 2\ 3)$, $\rho_2=(4\ 5\ 6)$ がそれぞれ３通りに表されるから，$\rho=\rho_1\rho_2=\rho_2\rho_1$ より，見掛け上 $2!\,3^2$ 通りの表し方がある．一般に，m 個の共通な文字を含まない k 項巡回置換の積である置換は見掛け上 $m!\,k^m$ 通りに表される．そこで，

例題 1. $\mathfrak{S}_n$ のタイプ $(m_1, m_2, \cdots\cdots, m_n)$ の共役類に属する元の個数は $n!/(m_1!\,1^{m_1}m_2!\,2^{m_2}\cdots\cdots m_n!\,n^{m_n})$.

証明　$h=m_1!\,1^{m_1}m_2!\,2^{m_2}\cdots\cdots m_n!\,n^{m_n}$ とおく．n 個の文字の順列の総数は $n!$ である．各順列で，はじめの m_1 個を１つずつかっこにくくり，つぎの $2m_2$ 個を２つずつかっこにくくるというようにすれば，見掛け上 $n!$ 個のタイプ $(m_1, m_2, \cdots\cdots, m_n)$ の置換が得られるが，上に述べたように同じ置換が h 個ずつ出てくるから，求める個数は $n!/h$ である．

この結果を使って，$\mathfrak{S}_4$, $\mathfrak{S}_5$ の共役類を求めれば，つぎのようになる．

$\mathfrak{S}_4$ の共役類

共役類	型	タイプ	代表元	個数
C_0	1 1 1 1	(4, 0, 0, 0)	e	1
C_1	1 1 2	(2, 1, 0, 0)	(1 2)	6
C_2	1 3	(1, 0, 1, 0)	(1 2 3)	8
C_3	2 2	(0, 2, 0, 0)	(1 2) (3 4)	3
C_4	4	(0, 0, 0, 1)	(1 2 3 4)	6

$\mathfrak{S}_4$ は 5 個の共役類に分かれ，類公式は $24=1+6+8+3+6$

$\mathfrak{S}_5$ の共役類

共役類	型	タイプ	代表元	個数
C_0'	1 1 1 1 1	(5, 0, 0, 0, 0)	e	1
C_1'	1 1 1 2	(3, 1, 0, 0, 0)	(1 2)	10
C_2'	1 1 3	(2, 0, 1, 0, 0)	(1 2 3)	20
C_3'	1 2 2	(1, 2, 0, 0, 0)	(1 2) (3 4)	15
C_4'	1 4	(1, 0, 0, 1, 0)	(1 2 3 4)	30
C_5'	2 3	(0, 1, 1, 0, 0)	(1 2) (3 4 5)	20
C_6'	5	(0, 0, 0, 0, 1)	(1 2 3 4 5)	24

$\mathfrak{S}_5$ は 7 個の共役類に分かれ，その類公式は

$$120 = 1 + 10 + 20 + 15 + 30 + 20 + 24$$

交代群 $\mathfrak{A}_n$ では，型が同じであっても共役とは限らない．$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の正規部分群であるから，$\mathfrak{A}_n$ は $\mathfrak{S}_n$ のいくつかの共役類の和集合であるが，$\mathfrak{A}_n$ に含まれている $\mathfrak{S}_n$ の共役類が $\mathfrak{A}_n$ で 2 つに分かれてしまうことがあるのである．たとえば，4 次交代群 $\mathfrak{A}_4$ には上記の C_0, C_2, C_3 が含まれているが，後に述べるように 8 個の元を含む C_2 はちょうど半分に分かれてしまう（実際 8 は $\mathfrak{A}_4$ の位数 12 を割り切らない）．

例題 2. $\mathfrak{A}_n(n\geqq 2)$ の元 σ に対し，$\sigma_1=(1\ 2)\sigma(1\ 2)^{-1}$ とおく．もしも σ と σ_1 が $\mathfrak{A}_n$ で共役ならば，$\mathfrak{S}_n$ における σ の属する共役類 $C(\sigma)$ は $\mathfrak{A}_n$ でもそのまま 1 つの共役類になっている．σ と σ_1 が $\mathfrak{A}_n$ で共役でなければ，$C(\sigma)$ は $\mathfrak{A}_n$ では 2 つの共役類 $C^*(\sigma)$ と $C^*(\sigma_1)$ とに分かれ，このとき，$C^*(\sigma)$ と $C^*(\sigma_1)$ は同じ個数の元からなる．

証明　$\mathfrak{S}_n=\mathfrak{A}_n+\mathfrak{A}_n\ (1\ 2)$ であるから，$C(\sigma)$ の元は $\tau\sigma\tau^{-1}$ か $\tau\,(1\ 2)\,\sigma\,(1\ 2)^{-1}\tau^{-1}$, $\tau\in\mathfrak{A}_n$ という形をしている．したがって，$C(\sigma)$ の元は σ に $\mathfrak{A}_n$ で共役な元の集合 $C^*(\sigma)$ と，σ_1 に $\mathfrak{A}_n$ で共役な元の集合 $C^*(\sigma_1)$ の和集合である．ゆえに，σ と σ_1 が $\mathfrak{A}_n$ で共役ならば，$C^*(\sigma)=C^*(\sigma_1)$ で，$C(\sigma)$ は $\mathfrak{A}_n$ でも 1 つの共役類をつくっている．もしも σ と σ_1 が $\mathfrak{A}_n$ で共役でなければ，$C^*(\sigma)\cap C^*(\sigma_1)=\phi$ で，$C(\sigma)$ は $C^*(\sigma)$

と $C^*(\sigma_1)$ に類別される．さて，$\tau\in\mathfrak{A}_n$ のとき，$\tau(1\ 2)=(1\ 2)\rho$, $\rho\in\mathfrak{A}_n$ であって，$\tau\sigma_1\tau^{-1}=\tau(1\ 2)\sigma(1\ 2)^{-1}\tau^{-1}=(1\ 2)\rho\sigma\rho^{-1}(1\ 2)^{-1}$ であるから，$\tau C^*(\sigma_1)\tau^{-1}=C^*(\sigma_1)\subset(1\ 2)C^*(\sigma)(1\ 2)^{-1}$ となり，$C^*(\sigma_1)$ の元の個数は $C^*(\sigma)$ の元の個数を越さない．他方，$\sigma=(1\ 2)\sigma_1(1\ 2)^{-1}$ であるから，$\tau\sigma\tau^{-1}=(1\ 2)\rho\sigma_1\rho^{-1}(1\ 2)^{-1}$ であって，$\tau C^*(\sigma)\tau^{-1}=C^*(\sigma)\subset(1\ 2)C^*(\sigma_1)(1\ 2)^{-1}$ となるから，$C^*(\sigma)$ の元の個数は $C^*(\sigma_1)$ の元の個数を越さない．したがって，これら２つの共役類の元の個数は等しい．

例題 3. 上の例題と同じ記号を使って，σ と σ_1 が $\mathfrak{A}_n$ で共役となるのは，σ の正規化群 $N(\sigma)$ が奇置換を含むとき，そのときに限る．

証明 $N(\sigma)$ が奇置換 ρ を含むとする．$(1\ 2)\rho\in\mathfrak{A}_n$ で，$(1\ 2)\rho\sigma\rho^{-1}(1\ 2)^{-1}=(1\ 2)(\rho\sigma\rho^{-1})(1\ 2)^{-1}=(1\ 2)\sigma(1\ 2)^{-1}=\sigma_1$. ゆえに σ と σ_1 は $\mathfrak{A}_n$ で共役である．逆に，σ と σ_1 が $\mathfrak{A}_n$ で共役とする．$\tau\sigma\tau^{-1}=\sigma_1$ となる $\mathfrak{A}_n$ の元 τ がとれるから，$\tau\sigma\tau^{-1}=\sigma_1=(1\ 2)\sigma(1\ 2)^{-1}$ より $(1\ 2)^{-1}\tau\sigma\tau^{-1}(1\ 2)=\sigma$ で，$(1\ 2)^{-1}\tau=\rho$ とおけば，ρ は奇置換であって，$\rho\sigma\rho^{-1}=\sigma$ であるから，$\rho\in N(\sigma)$.

さて，$\mathfrak{A}_4$ の共役類別を考えよう．$\mathfrak{S}_4$ の共役類で $\mathfrak{A}_4$ に含まれるものは C_0, C_2, C_3 である．$\sigma=(1\ 3)\ (2\ 4)$ は $(1\ 3)$ で変換しても変らないから，$(1\ 3)\in N(\sigma)$. したがって，C_3 は $\mathfrak{A}_4$ でも１つの共役類である．つぎに，$\tau(1\ 2\ 3)\tau^{-1}=(\tau(1)\tau(2)\tau(3))=(1\ 2\ 3)$ となる τ は巡回の順序を変えないから，それは $\sigma=(1\ 2\ 3)$ の巾しかない．したがって，$N(\sigma)=\langle\sigma\rangle$ で，$N(\sigma)$ はすべて偶置換からなるから，$C_2=C(\sigma)$ は $\mathfrak{A}_4$ で σ を含む共役類 $C^*(\sigma)$ と $\sigma_1=(1\ 2)\ (1\ 2\ 3)\ (1\ 2)^{-1}=(1\ 3\ 2)$ を含む共役類 $C^*(\sigma_1)$ とにちょうど半分ずつ分かれる．

$\mathfrak{A}_4$ の共役類はつぎの４つあり，各類の個数はつぎの通りである．

恒等置換の類	1 個	類公式
$(1\ 2\ 3)$ の類	4 個	$12=1+4+4+3$
$(1\ 3\ 2)$ の類	4 個	
$(1\ 2)\ (3\ 4)$ の類	3 個	

$\mathfrak{A}_4$ の部分群について注意すると，位数２の巡回群 $\langle(1\ 2)\ (3\ 4)\rangle$, 位数３の巡回群 $\langle(1\ 2\ 3)\rangle$, 位数４のアーベル群 $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4),$

(1 4)(2 3)} と，$\mathfrak{A}_4$ は位数 12 の約数 2, 3, 4 をそれぞれ位数にもつ部分群をもつが，位数 6 の部分群はもたない．なぜなら，そのような部分群 N は指数が 2 であるから，正規部分群であり，したがって，N は共役類の和集合である．N は単位元を含むから，N の位数 6 は上記の類公式の右辺の 1 を含めた部分和であるが，それは不可能である．

$\mathfrak{S}_5$ の共役類のうち，$\mathfrak{A}_5$ に入っているものは C_0', C_2', C_3', C_6' である．$\sigma=(1\ 2)(3\ 4)$ は $(1\ 2)$ で変換しても変らないから，$(1\ 2)\in N(\sigma)$ である．よって $C_3'=C(\sigma)$ は $\mathfrak{A}_n$ でもそのまま 1 つの共役類をつくっている（もっとも 15 は 2 で割り切れない）．また $(1\ 2\ 3)$ は $(4\ 5)$ で変換しても変らないから，$(4\ 5)\in N((1\ 2\ 3))$ であり，したがって $C_2'=C(1\ 2\ 3)$ も $\mathfrak{A}_5$ で 1 つの共役類をつくっている．つぎに，$\sigma=(1\ 2\ 3\ 4\ 5)$ と可換な τ，つまり $\tau\sigma\tau^{-1}=\sigma$ となる τ は，σ の巾しかないから，$N(\sigma)=\langle\sigma\rangle$ で，$N(\sigma)$ は偶置換だけからなっている．したがって，C_6' は σ を含む類 $C^*(\sigma)$ と，σ を $(1\ 2)$ で変換した $\sigma_1=(1\ 2)(1\ 2\ 3\ 4\ 5)(1\ 2)^{-1}=(2\ 1\ 3\ 4\ 5)=(1\ 3\ 4\ 5\ 2)$ を含む類 $C^*(\sigma_1)$ とに，ちょうど半分ずつ分かれる．

$\mathfrak{A}_5$ の共役類は 5 つあって，各類の元の個数はつぎの通り．

恒等置換の類	1 個	類公式
(1 2 3) の類	20 個	60=1+20+15+12+12
(1 2)(3 4) の類	15 個	
(1 2 3 4 5) の類	12 個	
(1 3 4 5 2) の類	12 個	

例題 4. $\mathfrak{A}_5$ は単純群である．

証明 N を $\mathfrak{A}_5$ の正規部分群とすれば，N はいくつかの共役類の和集合である．N は単位元を含むから，N の位数は上記類公式の右辺の 1 を含めた部分和である．そのような部分和は 1 か 60 でないかぎり 60 の約数でない．つまり，$N=\{e\}$ か $N=\mathfrak{A}_5$ で，ゆえに $\mathfrak{A}_5$ は単純群である．

注 $\mathfrak{A}_n(n\geqq 5)$ が単純群であることは p. 97 例題 4 で証明する．

問 題 2

1. 群 G の部分集合 M から生成された群 $\langle M\rangle$ は M を含むすべての部分群の共通部分である．したがって，$\langle M\rangle$ は M を含む最小の部分群である．

2. 群 G の部分群 H のすべての共役群の共通集合は正規部分群である．

3. 群 G の部分群の位数を m とする．位数 m の部分群が H 以外になければ，H は G の正規部分群である．

4. H, K が群 G の正規部分群で，$H\cap K=\{e\}$ ならば，H の元と K の元は可換である．

5. Hを群 G の有限部分群とする．HaH が唯一つの H を法とする左剰余類を含むだけならば，a は H の正規化群 $N(H)$ の元である．

6. Nは群 G の正規部分群，H は N を含む G の部分群とすれば，H/N は G/N の部分群である．逆に，$\bar{G}=G/N$ の部分集合，$\{hN\}=\bar{H}$ が $\bar{G}$ の部分群ならば，$H/N=\bar{H}$ となる G の部分群 H が存在する．とくに，$\bar{H}$ が $\bar{G}$ の正規部分群であれば，H は G の正規部分群である．

7. 0でない実数全体のつくる乗法群 $\boldsymbol{R}^*$ の指数有限な部分群は，正の実数全体のつくる部分群 P だけである．また，実数全体のつくる加法群 $\boldsymbol{R}$ は指数有限の真の部分群をもたない．また $\boldsymbol{R}$ と P は同型である．

8. K は有理数全体か実数全体か複素数全体とする．K の数を成分とする n 次の正則行列（行列式が0でない行列）の全体は行列の積に関して1つの群をつくる．これを $GL(n, K)$ で表し，K 上の n 次の**一般1次変換群**という．また，$SL(n, K)=\{A|A\in GL(n, K),\ \det A=1\}$ は $GL(n, K)$ の正規部分群である．$SL(n, K)$ を K 上の n 次の**特殊1次変換群**という．

9. $SL(2, \boldsymbol{R})$ の中心は $\{E, -E\}$ である．ここで，E は2次の単位行列を表す．また，つぎの集合 T は $SL(2, \boldsymbol{R})$ の部分群であるが，正規部分群ではない．

$$T=\left\{\begin{pmatrix}1 & \tau\\ 0 & 1\end{pmatrix},\ \tau\in\boldsymbol{R}\right\}$$

注　$n\geqq 2$ のとき，$SL(n, K)$ の中心 Z は有限群 $\{\alpha E,\ E$ は単位行列，$\alpha\in K,\ \alpha^n=1\}$ であって，$SL(n, K)/Z$ は真の正規部分群を含まない，すなわち，単純群であることが知られている（巻末文献〔3〕の第I巻参照）．

10. $6 \leqq n$ である偶数 n に対し，位数 n の非可換群をつくれ.

11. a, b を生成元とし,

$$a^4 = e, \quad a^2 = b^2, \quad bab^{-1} = a^{-1}$$

という関係で定義された群 Q について，つぎのことを示せ.

(1) Q は位数 8 の非可換群である.

(2) Q のすべての部分群は正規部分群である.

(3) Q は 4 元数群（問題 1 の 8 をみよ）と同型である.

12. つぎの行列 A, B で生成された群は 4 元数群と同型である.

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{ここで } i = \sqrt{-1}$$

13. a, b, c を生成元とし，関係

$$a^2 = b^2 = c^2, \quad a^4 = e, \quad ab = c, \quad bc = a, \quad ca = b$$

で定義された群は 4 元数群と同型である.

14. 関係

$$a^{2^{n-1}} = e, \quad b^2 = a^{2^{n-2}}, \quad bab^{-1} = a^{-1} \quad (n \geqq 3)$$

をみたす a, b で生成された群 Q_n を**一般4元数群**という．とくに，$n=3$ のときが，先に述べた 4 元数群である．Q_n の位数は 2^n である.

15. G は $x^2 = y^2 = e$ をみたす x, y で生成された非可換群とすると，G は指数 2 の部分群を含む．さらに，もしも G の位数が $2n$ $(n \geqq 3)$ であれば，G は n 次 2 面体群 D_n と同型である.

16. N は群 G の，指数が有限な正規部分群，H は G の有限部分群とする．もしも，$|G:N|$ と $|H|$ が互いに素であれば，$H \subset N$.

17. 有限群 G の正規部分群 N の位数 m と指数 r が互いに素であれば，位数が m の約数である G の部分群はすべて N に含まれる.

18. N は群 G の有限正規部分群，H は G の，指数が有限な部分群とする．もしも，$|G:H|$ と $|N|$ が互いに素であれば，$N \subset H$.

19. H_1, H_2, K は群 G の部分群で，$H_1 \subset H_2$ であれば

$$H_1K \cap H_2 = H_1(K \cap H_2)$$

20. H_1, H_2, K は群 G の部分群で，$H_1 \subset H_2$, $H_1 \cap K = H_2 \cap K$, $H_1K = H_2K$ であれば $H_1 = H_2$.

21. 有限群 G の部分群 H_1, H_2 に対し，$K_1 = H_1 \cap H_2$, K_2 は H_1, H_2 で生成された

群 $\langle H_1, H_2\rangle$ とすれば，$|H_1||H_2|\leqq|K_1||K_2|$. 等号は $K_2=H_1H_2$ のとき，そのときに限る.

22. H が有限群 G の真の部分群のとき，H のどの共役群にも含まれないような G の元が存在する.

23. H が群 G の指数有限の部分群のとき，H は G の指数が有限である正規部分群を含む.

24. H が群 G の指数有限の真の部分群のとき，H のどの共役群にも含まれない G の元が存在する.

25. H が群 G の指数が有限 n の部分群であるとき，

$$G = a_1H + \cdots\cdots + a_nH = Ha_1 + \cdots\cdots + Ha_n$$

であるような n 個の元 $a_1, \cdots\cdots, a_n$ が存在する.

3

準同型・同型

3-1 準同型・同型

3-1-1 準同型・同型

群 G から群 G' への写像 φ が演算を保存するとき，すなわち，G の任意の元 a, b に対して，

$$\varphi(ab) = \varphi(a)\varphi(b)$$

がつねに成り立つとき，φ を G から G' への**準同型写像**または単に**準同型**という．とくに，φ が G から G' の上への写像，すなわち $\varphi(G)=G'$ であるとき，G は G' に準同型であるといい，記号 $G \sim G'$ で表す．

例題 1. $\varphi: G \longrightarrow G'$ が準同型であれば，G の単位元 e には G' の単位元 e' が対応し，G の元 a の逆元には $\varphi(a)$ の逆元が対応する：

$$\varphi(e) = e', \quad \varphi(a^{-1}) = \varphi(a)^{-1}$$

証明 $ee=e$ より，$\varphi(e)\varphi(e)=\varphi(ee)=\varphi(e)$ であるから，$\varphi(e)$ は G' の単位元である．$aa^{-1}=e$ より，$\varphi(a)\varphi(a^{-1})=\varphi(aa^{-1})=\varphi(e)$．したがって，$\varphi(a^{-1})=\varphi(a)^{-1}$．

例 1. 整数の加法群 $\boldsymbol{Z}$ において，$\varphi(n)=2n$ とすれば，φ は $\boldsymbol{Z}$ から $\boldsymbol{Z}$ の中への準同型である．

例 2. 群 G の1つの元を a とする．整数 n に対し $\varphi(n)=a^n$ とすれば，$\varphi(n+m)=a^{n+m}=a^n a^m=\varphi(n)\varphi(m)$ であるから，φ は加法群 $\boldsymbol{Z}$ から G への準同型である．

例 3. n 次対称群 $\mathfrak{S}_n \ni \sigma$ が偶置換のとき $\varphi(\sigma)=1$，奇置換のとき $\varphi(\sigma)=-1$ とおけば，φ は $\mathfrak{S}_n$ から群 $\{1, -1\}$ の上への準同型である．

例題 2. $\varphi: G \longrightarrow G'$ を準同型，H を G の部分群とすれば，$\varphi(H)$ は

G' の部分群である．とくに，$\varphi(G)<G'$．もしも $H\lhd G$ であれば，$\varphi(H)$ は $\varphi(G)$ の正規部分群である．

証明　$a, b\in H$ であれば，$\varphi(a)\varphi(b)^{-1}=\varphi(a)\varphi(b^{-1})=\varphi(ab^{-1})\in\varphi(H)$ であるから，$\varphi(H)<G$．$H\lhd G$ ならば，$\varphi(G)$の元 a' は $a'=\varphi(a)$, $a\in G$, と書けるから，$a'\varphi(H)a'^{-1}=\varphi(a)\varphi(H)\varphi(a^{-1})=\varphi(aHa^{-1})=\varphi(H)$ となる．したがって，$\varphi(H)\lhd\varphi(G)$．

問 1.　巡回群の準同型による像は巡回群である．

例題 3.　$\varphi: G\longrightarrow G'$ を準同型とするとき，G' の単位元 e' の原像

$$\varphi^{-1}(e')=\{x|x\in G, \varphi(x)=e'\}$$

は G の正規部分群である．これを φ の核といって，$\mathrm{Ker}\,\varphi$ で表す．

証明　$\varphi(x)=\varphi(y)=e'$ ならば，$\varphi(xy)=\varphi(x)\varphi(y)=e'e'=e'$ であり，$\varphi(x^{-1})=\varphi(x)^{-1}=e'^{-1}=e'$ であるから，$x, y\in\mathrm{Ker}\,\varphi$ ならば，$xy, x^{-1}\in\mathrm{Ker}\,\varphi$ となって，$\mathrm{Ker}\,\varphi<G$．つぎに，G の任意元 a, $\mathrm{Ker}\,\varphi$ の任意元 x に対して，$\varphi(axa^{-1})=\varphi(a)\varphi(x)\varphi(a^{-1})=\varphi(a)\varphi(a^{-1})=\varphi(aa^{-1})=e'$ であるから，$\mathrm{Ker}\,\varphi\lhd G$．

$\varphi: G\sim G'$ のとき，G' の部分集合 M' に対して，$\varphi^{-1}(M')$ は φ の核 N を法とした G の剰余類の和集合である．なぜなら，$\varphi(x)\in M'$ であれば，N の任意元 a に対し $\varphi(ax)=\varphi(a)\varphi(x)=\varphi(x)\in M'$ であるから，$Nx\subset\varphi^{-1}(M')$ であり，したがって，$\varphi^{-1}(M')=\bigcup Nx$．ここで，$x$ は $\varphi^{-1}(M')$ 全体を動く．とくに，G の部分集合 M の像を M' とすれば，$\varphi^{-1}(M')=NM=MN$．実際，$\varphi(x)\in\varphi(M)$とすれば，$\varphi(x)=\varphi(y)$, $y\in M$, であるから，$\varphi(xy^{-1})=e$ となり，$xy^{-1}\in N$．したがって，$x\in Ny\subset NM$．$\therefore$　$\varphi^{-1}(M')\subset NM$．一方，$\varphi(NM)=\varphi(N)\varphi(M)=\varphi(M)=M'$ であるから，$NM\subset\varphi^{-1}(M')$．

例題 4.　$\varphi: G\longrightarrow G'$ を準同型とし，H を G の部分群とすれば，$\varphi(H)=H'$ の原像 $\varphi^{-1}(H')$は$NH=HN$．ここで，$N=\mathrm{Ker}\,\varphi$．

証明　上に述べたことから，ただちに出る．

例題 5.　$\varphi: G\longrightarrow G'$ を準同型とする．H' が G' の部分群のとき，$\varphi^{-1}(H')$ は G の部分群である．また，H' が G' の正規部分群ならば，$\varphi^{-1}(H')$ は G の正規部分群である．

証明　$H=\varphi^{-1}(H')\ni a, b$ なら，$\varphi(ab)=\varphi(a)\varphi(b)\in H'$ であるから，$ab\in H$．また，

$\varphi(a^{-1})=\varphi(a)^{-1}\in H'$ であるから，$a^{-1}\in H$. したがって $H<G$. また $H'\lhd G'$ のときは，G の任意元 a に対し，$\varphi(aHa^{-1})=\varphi(a)\varphi(H)\varphi(a)^{-1}\subset\varphi(a)H'\varphi(a)^{-1}=H'$ であるから，$aHa^{-1}\subset H$ となり，したがって，$H\lhd G$.

例 4. N を群 G の正規部分群とする．G から G/N への写像

$$\varphi(a) = aN = Na$$

は，$\varphi(ab)=abN=aNbN=\varphi(a)\varphi(b)$ であり，$\varphi(G)=G/N$ であるから，G から G/N の上への準同型である．この準同型 φ を G から G/N への**自然な**または**標準的な準同型**という．このとき $\mathrm{Ker}\,\varphi=N$ である．

$\varphi: G\longrightarrow G/N$ を自然な準同型，$G>H>N$ とすれば，$H'=\varphi(H)=H/N$ は $\bar{G}=\varphi(G)=G/N$ の部分群であり，とくに $H\lhd G$ であれば，$H'\lhd\bar{G}$.

逆に，H' を $\bar{G}$ の部分群とすれば，$H=\varphi^{-1}(H')$ は G の，N を含む部分群であり，とくに $H'\lhd\bar{G}$ であれば，$H\lhd G$. このように G から G/N への自然な準同型によって，N を含む G の部分群と G/N の部分群は1対1に対応し，とくに N を含む G の正規部分群と，G/N の正規部分群とが互いに対応する．

問 2. φ を G から G/N への自然な準同型，H を G の部分群とすれば，$\varphi(H)=HN/N$ である．

3-1-2 準同型定理・同型定理

先に1-5節で述べたように，準同型 $\varphi: G\longrightarrow G'$ は1対1であるとき，つまり，任意の2つの異なる元 $a\neq b$ に対して，$\varphi(a)\neq\varphi(b)$ であるとき，G から G' への同型であるという．$\forall a, b, a\neq b, \varphi(a)\neq\varphi(b)$ ということは，$\varphi(a)=e'$（G' の単位元）となる G の元 a は単位元に限るということと同じである．とくに，φ が G から G' の上への同型であるとき，G と G' は**同型である**といい，記号 $\varphi: G\cong G'$ で表す．

［定理 1］　**（準同型定理）**

φ を群 G から群 G' の上への準同型とするとき，N を φ の核とすれば，$G/N\cong G'$.

[証明]　e' を G' の単位元とする．G の2つの元 a, b について，$\varphi(a)=\varphi(b) \Leftrightarrow \varphi(a)^{-1}\varphi(b)=\varphi(a^{-1}b)=e' \Leftrightarrow a^{-1}b\in N \Leftrightarrow b\in aN$. したがって，$aN\neq bN$ であれば，$\varphi(a)\neq\varphi(b)$. $\bar{\varphi}: \bar{a}=aN \longrightarrow a'=\varphi(a)$ とすれば，$\bar{\varphi}$ は1対1であり，φ が上への写像であるから，G/N から G' の上への写像でもある．さて，$\bar{\varphi}(\bar{a}\bar{b})=\bar{\varphi}(abN)=\varphi(ab)=\varphi(a)\varphi(b)=\bar{\varphi}(aN)\bar{\varphi}(bN)=\bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b})$ であるから，$\bar{\varphi}$ は，同型対応である．

例 1.　G が位数 n の巡回群のとき，加法群 $\boldsymbol{Z}$ の，n で生成された巡回部分群を N とすれば，$\boldsymbol{Z}/N\cong G$.

問 1.　G を無限巡回群，G' を巡回群とすると，G から G' の上への準同型が存在する．この準同型の核 N を求めよ．

例 2.　正8面体の向かい合った頂点を結ぶ3つの対称軸に番号をつけて1, 2, 3とする．正8面体群に属する回転によって，1, 2, 3の置換が引き起こされる．1のまわりの90°の回転では置換(2, 3)が引き起こされる．一般に，i, $1\leqq i\leqq 3$ のまわりの90°の回転 f_i は置換 $\sigma_i=(k, j)$, $i\neq j, k$ を引き起こす．したがって，G は，$\mathfrak{S}_3$ の上に準同型にうつされる．この準同型を φ とすれば，φ の核は，$|G|=24$, $|\mathfrak{S}_3|=6$ より，位数4である．一方，$\tau_i=f_i^2$ とおくと，τ_i は恒等置換を引き起こす．よって N は $e, \tau_1, \tau_2, \tau_3$ の4つの回転からなる．ここで，$\tau_1\tau_2=\tau_2\tau_1=\tau_3$, $\tau_1^2=\tau_2^2=e$ であるから，N はクラインの4元数群と同型である．

[定理 2]　**(第1同型定理)**

φ を群 G から群 G' の上への準同型とし，N' を G' の正規部分群とすれば，N' の原像 $N=\varphi^{-1}(N')$ は G の正規部分群であり，$G/N\cong G'/N'$ である．

[証明]　前半は p. 66 例題5である．ϕ を $G'\longrightarrow G'/N'$ という自然な準同型とする．φ と ϕ の積 $\phi\varphi$ によって $G\overset{\varphi}{\longrightarrow}G'\overset{\phi}{\longrightarrow}G'/N'$ と G は G'/N' の上に準同型にうつされる．実際 $a, b\in G$ のとき，$a'=\varphi(a)$, $b'=\varphi(b)$ とすれば，$\phi\varphi(ab)=\phi(\varphi(ab))=\phi(a'b')=a'Nb'N=\phi(a')\phi(b')=\phi\varphi(a)\phi\varphi(b)$. $\mathrm{Ker}\,\phi\varphi=\{x|x\in G, \phi\varphi(x)=N'\}=\{x|x\in G, \varphi(x)N'=N'\}=\{x|x\in G, \varphi(x)\in N'\}=\varphi^{-1}(N')=N$.

[系]　H, N がともに群 G の正規部分群で，$H\supset N$ であれば，

$$(G/N)/(H/N)\cong G/H$$

[証明]　$G'=G/N$, $H'=H/N$ とすれば，H' は G' の正規部分群である．$\varphi: G\longrightarrow G'=G/N$ を自然な準同型とすると，$\varphi(H)=H/N=H'$ で，$\varphi^{-1}(H')=HN=H$.

したがって，第1同型定理によって $G/H \cong G'/H'$ である．

［定理 3］　**（第2同型定理）**

H を群 G の部分群，N を G の正規部分群とすれば，

$$HN/N \cong H/H \cap N$$

［証明］　$\varphi : a \longmapsto aN$ $(a \in G)$ によって，G は G/N の上に準同型にうつされ，部分群 H は HN/N の上にうつされる．φ を H 上に制限したものを φ' で表せば，$\mathrm{Ker}\,\varphi' = \{h \mid h \in H,\ \varphi'(h) = hN = N\} = \{h \mid h \in H,\ h \in N\} = H \cap N$．したがって，準同型定理によって，$H/H \cap N \cong HN/N$．

例題 1.　4次対称群 $\mathfrak{S}_4$ において，つぎの部分集合 V は正規部分群である：$V = \{e, (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}$
また，$\mathfrak{S}_4/V \cong \mathfrak{S}_3$ である．

証明　たとえば，$(1\ 2)\ (3\ 4)\ (1\ 3)\ (2\ 4) = (1\ 4)\ (2\ 3)$，$(1\ 3)\ (2\ 4)\ (1\ 2)\ (3\ 4) = (1\ 4)\ (2\ 3)$．$V$ の他の2つの元 $\neq e$ の組についても同様なことがいえて，V はクラインの4元群と同型な部分群であることがわかる．また，$\mathfrak{S}_4$ の任意の元 σ に対して，$\sigma(1\ 2)\ (3\ 4)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$．$(i\ j)\ (k\ l)$，$i, j, k, l$ は互いに異なる，という形の元はすべて V に入るから，$\sigma(1\ 2)\ (3\ 4)\sigma^{-1} \in V$．$V$ の他の元についても同様であるから，$\sigma V \sigma^{-1} \subset V$．$\therefore$　$V \lhd G$．いま，$\mathfrak{S}_4$ の元のうち，4を動かさないもの全体 H は，$\mathfrak{S}_3$ と同型な部分群をつくり，$H \cap V = \{e\}$．$\therefore$　$HV/V \cong H/H \cap V \cong \mathfrak{S}_3$．$|V| = 4$，$|\mathfrak{S}_3| = 6 = |HV : V|$ であるから，$|HV| = 24$．したがって，$HV = \mathfrak{S}_4$ となり，ゆえに，$\mathfrak{S}_4/V \cong \mathfrak{S}_3$．

3-2 自 己 同 型

群 G から G 自身の上への同型を，G の**自己同型**という．G の自己同型の全体を $A(G)$ で表すと，$A(G)$ は1つの群をつくる．実際，恒等写像 $I : x \longmapsto x$, $\forall x \in G$，は G の自己同型であるから，$I \in A(G)$ であり，$\sigma \in A(G)$ のとき，$\sigma : x \longmapsto x'$ の逆写像 $\sigma^{-1} : x' \longmapsto x$ は G を G 自身に1対1にうつし，$\sigma^{-1}(x'\ y') = \sigma^{-1}((x\,y)') = xy = \sigma^{-1}(x')\sigma^{-1}(y')$ であるから，$\sigma^{-1} \in A(G)$．さらに，$\sigma, \tau \in A(G)$ ならば，$\sigma\tau$ は G を G 自身に1対1にうつし，

$\sigma\tau(x\ y)=\sigma(\tau(x\ y))=\sigma(\tau(x)\tau(y))=\sigma(\tau(x))\sigma(\tau(y))=\sigma\tau(x)\sigma\tau(y)$ であるから，$\sigma\tau\in A(G)$ となる．したがって，$A(G)$ は群をつくる．この $A(G)$ を G の**自己同型群**という．

G の各元 x を axa^{-1} にうつす写像 σ_a は G の変換である．なぜなら，G の任意の異なる元 x, y について $axa^{-1}\neq aya^{-1}$ であり，また，G の任意の元 z は $a^{-1}za$ の σ_a による像であるから．ところで，

$$\sigma_a(xy)=axya^{-1}=axa^{-1}aya^{-1}=\sigma_a(x)\sigma_a(y)$$

であるから，σ_a は G の自己同型である．σ_a を a で引き起こされた G の**内部自己同型**という．

[定理 4]　群 G の自己同型群を $A(G)$，$G\ni a$ による内部自己同型を $\sigma_a: x\longmapsto axa^{-1}$ とすると，

(1)　対応 $\sigma: a\longmapsto\sigma_a$ は G から $A(G)$ への準同型である．

(2)　σ による G の像を $I(G)$とすると，$I(G)$は G の自己同型の全体である．$I(G)$は $A(G)$の正規部分群である．$I(G)$をGの**内部自己同型群**という．

(3)　σ の核は G の中心 Z_G である．したがって $G/Z_G\cong I(G)$.

[証明]　(1)　$\sigma_{ab}(x)=abx(ab)^{-1}=a(bxb^{-1})a^{-1}=\sigma_a(\sigma_b(x))=\sigma_a\sigma_b(x)\quad\forall x\in G$ より，$\sigma_{ab}=\sigma_a\sigma_b$ であるから，対応 $\sigma: a\longmapsto\sigma_a$ は G から $A(G)$ への準同型である．

(2)　準同型像 $I(G)$ は $A(G)$ の部分群である．明らかに $I(G)$ は G の元による内部自己同型の全体である．いま，$\tau\in A(G)$ とすれば，$\tau\sigma_a\tau^{-1}(x)=\tau\sigma_a(\tau^{-1}(x))=\tau(a\tau^{-1}(x)a^{-1})=\tau(a)x\tau(a^{-1})=\tau(a)x\tau(a)^{-1}\quad\forall x\in G$ であるから，$\tau\sigma_a\tau^{-1}=\sigma_{\tau(a)}$ であって，$\tau I(G)\tau^{-1}\subset I(G)$．ゆえに，$I(G)\lhd A(G)$.

(3)　$\sigma_a(x)=axa^{-1}=x\quad\forall x\in G\Leftrightarrow a\in Z_G$ であるから，σ の核は Z_G であり，したがって $G/Z_G\cong I(G)$.

　例 1.　G は位数 g のアーベル群とする．n と g が互いに素であれば，対応 σ：$a\longmapsto a^n$ は G の自己同型である．なぜなら，まず $(ab)^n=a^nb^n$ であるから，σ は準同型であり，$a^n=e$ となるのは，$(g, n)=1$ であるから，$a=e$ のときに限るから，σ は1対1である．G は有限集合であるから，σ は G から G の上への写像である．

例題 1. 位数が n の巡回群 G の自己同型群は n を法とする既約剰余類群 Z_n^* と同型である．したがって，$A(G)$ の位数は $\varphi(n)$ である．

証明 G の自己同型 σ によって，位数 r の元は同じく位数 r の元にうつり，とくに G の生成元の像はまた生成元である．a を G の生成元とすれば，$\sigma(a)=a^r$ は G の生成元であるから，r と n は互いに素であり，r は n を法として定まる．したがって，σ に対して法 n の既約剰余類 $C(r)$ が対応する．逆に，$C(r)$ を法 n の既約剰余類とすれば，$\sigma: a\longmapsto a^r$ は，a^r が G の生成元であるから，G の自己同型となる（例 1）．したがって，G の自己同型と法 n の既約剰余類が 1 対 1 に対応する．いま $\sigma\longmapsto C(r)$，$\tau\longmapsto C(s)$ とすれば，$\sigma\tau(a)=\sigma(a^s)=a^{sr}$ であるから，$\sigma\tau\longmapsto C(rs)=C(r)C(s)$ となって，対応 $\sigma\longmapsto C(r)$ は G の自己同型群 $A(G)$ から Z_n^* の上への同型となる．

問 1. 位数 3 の巡回群の自己同型群も，位数 4 の巡回群の自己同型群もともに位数 2 の巡回群である．

問 2. 位数が素数 p の巡回群の自己同型群は位数が $p-1$ の巡回群である．

問 3. p を素数，n を自然数とするとき，$n|\varphi(p^n-1)$ である．

例題 2. 4 次対称群 $\mathfrak{S}_4$ の自己同型群は $\mathfrak{S}_4$ と同型である．

証明 はじめに $\mathfrak{S}_n(n\geqq3)$ の中心は単位群であることをいう．($n=2$ のとき，$\mathfrak{S}_2$ は位数 2 の巡回群で，中心は $\mathfrak{S}_2$)．$\mathfrak{S}_n\ni\sigma$ が長さ $s<n$ の巡回置換 $(a_1a_2\cdots\cdots a_s)$ ならば，$(a_sa_n)\sigma(a_sa_n)^{-1}=(a_1a_2\cdots\cdots a_n)\neq\sigma$，$\sigma\notin$ 中心 Z．$s=n$ のときは $(a_1\ a_2)\sigma(a_1\ a_2)^{-1}=(a_2a_1\cdots\cdots a_s)\neq\sigma$，$\sigma\notin \boldsymbol{Z}$．つぎに，$\sigma=(a_1\cdots\cdots a_s)\ (a_{s+1}\cdots\cdots)$ と共通の文字を含まぬ巡回置換の積であれば，$(a_sa_{s+1})\sigma(a_sa_{s+1})^{-1}=(a_1\cdots\cdots a_{s+1})\ (a_s\cdots\cdots)\neq\sigma$，$\sigma\notin \boldsymbol{Z}$．したがって中心 $\boldsymbol{Z}=\{e\}$．ゆえに，$I(\mathfrak{S}_4)=I(\mathfrak{S}_4)/\boldsymbol{Z}\cong\mathfrak{S}_4$ であるから，結局，$A(\mathfrak{S}_4)=I(\mathfrak{S}_4)$ を示せばよい．$\mathfrak{S}_4$ は，共役類の分類からわかるように，位数が 3 の元を 8 個含み，位数が 3 の部分群は，$P_1=\langle(2\ 3\ 4)\rangle$，$P_2=\langle(1\ 3\ 4)\rangle$，$P_3=\langle(1\ 2\ 4)\rangle$，$P_4=\langle(1\ 2\ 3)\rangle$ の 4 つある．これら 4 つの部分群は，たとえば，$(1\ 2)\ P_1(1\ 2)^{-1}=P_2$ のように，互いに共役で，$xP_ix^{-1}=P_j$，ここで，$x=(i\ j)$．$\mathfrak{S}_4$ の自己同型は位数 3 の部分群を位数 3 の部分群にうつすので，これら 4 つの群の置換を引き起こすから，$\mathfrak{S}_4$ の自己同型に，$\mathfrak{S}_4$ の元が対応する．もしも $A(\mathfrak{S}_4)\ni\sigma$ に対して，$\sigma P_k=P_k$，$\forall k$，であれば，任意の互換 $x=(i,\ j)$ に対して，$xP_ix^{-1}=P_j$ より，$\sigma(x)P_i\sigma(x)^{-1}=P_j$ となる．$\sigma(x)$ も互換であるから，$\sigma(x)=x$．したがって $\sigma(z)=z\quad\forall z\in\mathfrak{S}_4$．したがって σ は自己同型 I に等しい．ゆえに，$A(\mathfrak{S}_4)\ni\sigma,\ \tau,\ \sigma\neq\tau$，であれば，$\sigma,\ \tau$ に対応する置換 $\varphi(\sigma)$ と $\varphi(\tau)$

は異なるから，φ は1対1対応である：$A(\mathfrak{S}_4)\cong\varphi A(\mathfrak{S}_4)\subset\mathfrak{S}_4$．したがって，$|A(\mathfrak{S}_4)|\leqq 4!$．一方，$A(\mathfrak{S}_4)\supset I(\mathfrak{S}_4)\cong\mathfrak{S}_4$ であるから，$|A(\mathfrak{S}_4)|=4!$ となる．したがって，$A(\mathfrak{S}_4)=I(\mathfrak{S}_4)$ となる．

問 4.　3次対称群 $\mathfrak{S}_3$ の自己同型群 $A(\mathfrak{S}_3)$ は $\mathfrak{S}_3$ と同型である．($\mathfrak{S}_3$ は $(1\ 2)$, $(1\ 3)$, $(2\ 3)$ から生成され，$\mathfrak{S}_3$ の自己同型は，これら3個の元の置換を引き起こすことに注目せよ)．

問 5.　3次交代群 $\mathfrak{A}_3$ の自己同型群は位数2の巡回群である．

問 6.　4次交代群 $\mathfrak{A}_4$ の自己同型群は $\mathfrak{S}_4$ と同型である．

($\mathfrak{A}_4$ は，共役類の分類からわかるように，位数が3の元を8個，位数が2の元を3個含む．また，$\mathfrak{S}_4$ の自己同型はすべて $\mathfrak{S}_4$ の元 σ で引き起こされる内部自己同型で，それはまた $\mathfrak{A}_4$ の自己同型である)．

問 7.　$\mathfrak{A}_4$ の内部自己同型群 $I(\mathfrak{A}_4)$ は $\mathfrak{A}_4$ と同型である．

注　$\mathfrak{S}_2$ は位数2の巡回群で，$A(\mathfrak{S}_2)=\{e\}$．また，$A(\mathfrak{A}_2)=\{e\}$．$\mathfrak{S}_3$ については，$A(\mathfrak{S}_3)=I(\mathfrak{S}_3)\cong\mathfrak{S}_3$, $A(\mathfrak{A}_3)$ は位数2の巡回群，$I(\mathfrak{A}_3)=\{e\}$．$n>3$ のときには，つぎのことがわかっている．

$n>3$, $n\neq 6$ のとき，

$$A(\mathfrak{S}_n)=I(\mathfrak{S}_n)\cong\mathfrak{S}_n,\qquad A(\mathfrak{S}_n)=A(\mathfrak{A}_n)$$

$n=6$ のときは，

$$A(\mathfrak{S}_6)=A(\mathfrak{A}_6),\ \ I(\mathfrak{S}_6)\cong\mathfrak{S}_6$$
$$|A(\mathfrak{S}_6):I(\mathfrak{S}_6)|=2$$

[定理 5]　$n\geqq 3$, $n\neq 6$ のとき，$\mathfrak{S}_n$ の自己同型はすべて内部自己同型である．したがって，$A(\mathfrak{S}_n)\cong\mathfrak{S}_n$．

[証明]　$\mathfrak{S}_n$ の元は互換の積であるから，φ を $\mathfrak{S}_n$ の任意の自己同型とするとき，任意の互換 $(a\ b)$ に対して，$\varphi(a\ b)=\sigma(a\ b)\sigma^{-1}=(\sigma(a), \sigma(b))$ となるような $\mathfrak{S}_n$ の元 σ がとれることをいえばよい．そのために，はじめに，$\mathfrak{S}_n$ の互換の φ による像がまた互換であることを示す．$\mathfrak{S}_n$ の位数2の元は，共通の文字を含まない互換の積に表される置換であり，またそれだけに限る．k 個の共通の文字を含まない互換の積である元は全体として1つの共役類をつくる．これを C_k で表す．とくに，C_1 はすべての互換の集合である．一般に，群の自己同型は元の位数を変えず，共役類を共役類にうつすから，φ は C_1 をある C_k $(k\geqq 1)$ にうつす．$n=3$ のときは C_1 は位数が2の元

の全体であるから，$\varphi(C_1)=C_1$．$n\geqq 4$, $n\neq 6$, のとき $\varphi(C_1)=C_1$ を示せばよい．C_1 の元の個数は $n(n-1)/2$, $C_k(k\geqq 2)$ の元の個数は，p. 58, 例題1で示したように，$n!/\{(n-2k)!\,k!\,2^k\}$ である．$\varphi(C_1)=C_k$, $k\geqq 2$ とすれば，$n(n-1)/2=n!/\{(n-2k)!\,k!\,2^k\}$ より，$(n-2)\cdots\cdots(n-2k+1)=k!\,2^{k-1}$ となる．この等式は $n\geqq 2k$ であるから，$k=2$ のときは成り立たない．$k=3$ のときは $n=6$ なら成り立つ．$k\geqq 4$ であれば，$n=2k$ のとき左辺は最小で，そのときすでに左辺の方が大きく，$n\geqq 2k$ ならば，左辺は右辺より大きい．したがって，$\varphi(C_1)=C_k$, $k\geqq 2$, ということはない．

つぎに，任意の文字 a に対し，a を含む任意の互換の φ による像は1つの決まった文字 a' を含む互換の全体であることを示す．$\varphi(ab)=(b'b'')$, $\varphi(ac)=(c'c'')$ で，b', b'', c', c'' がすべて互いに異なれば，$\varphi(abc)=\varphi((ac)(ab))=(c'c'')(b'b'')$ となり，位数3の元が位数2の元にうつることになるから，b', b'' の一方は，c', c'' のいずれかと一致する．したがって，$n=3$ のときは主張は確かめられた．$n\geqq 4$ のときはつぎのようなことが起こり得る．$\varphi(ab)=(a'b')$, $\varphi(ac)=(a'c')$, $\varphi(ad)=(b'c')$．しかし，このときは，$\varphi(abcd)=\varphi((ad)(ac)(ab))=(b'c')(a'c')(a'b')=(a'c')$ で，位数4の元が位数2の元にうつることになるから，実際にはこの場合は起きない．以上で，a を含む互換の φ による像は1つの文字 a' を含む互換であることがわかったが，a を含む互換も a' を含む互換も同数 $(n-1)$ 個ずつあるから，a' を含む任意の互換は，a を含むある互換の φ による像になっている．

さて，任意の互換 (ab) に対し，$\varphi(ab)$ は，a, b に対して上記のようにして定まる文字 a', b' を含むから，互換 $\varphi(ab)=(a'b')$．対応 $\sigma: a\longmapsto a'$ は，$a, b, \cdots\cdots$ 上の置換であるから，$\sigma\in\mathfrak{S}_n$ であって，求めるように $\varphi(ab)=(a'b')=(\sigma(a), \sigma(b))=\sigma(ab)\sigma^{-1}$ となる．

問 題 3

1. 0でない実数全体のつくる乗法群 $\boldsymbol{R}^*$ は実数の加法群 $\boldsymbol{R}$ と同型でない．
2. φ は群 G から群 G' の上への準同型とし，H' を G' の部分群，H を H' の φ による原像とする．$\{a_i\}$ が G の H を法とする完全右代表系ならば，$\{\varphi(a_i)\}$ は G' の H' を法とする完全右代表系である．したがって，$|G:H|=|G':H'|$ である．
3. H, G_1, G_2 は群 G の部分群で，G_2 は G_1 の正規部分群であれば，$G_1\cap H/G_2\cap H$ は G_1/G_2 の部分群に同型である．

4. Cを群Gの1つの共役類とする. σをGの自己同型とすれば, Cの像$\sigma(C)=\{\sigma x|x\in C\}$は$G$の共役類である.

5. 群Gの各共役類をそれぞれ自身にうつすようなGの自己同型の全体は, Gの自己同型群$A(G)$の正規部分群である.

6. 対応$x\longmapsto x^{-1}$が群Gの自己同型であれば, Gはアーベル群である.

7. 無限巡回群の自己同型は恒等写像$x\longmapsto x$か, $x\longmapsto x^{-1}$の2つしかない.

8. 位数4の非巡回群, クラインの4元群, の自己同型群は$\mathfrak{S}_3$と同型である.

4

直積・アーベル群・可解群

4-1 直　　積

4-1-1 与えられた群の直積

第2章では，1つの群 G とその正規部分群 N とから剰余群とよばれる新しい群 G/N をつくることを述べたが，ここでは，いくつかの与えられた群から，その各々を部分群として含むような群を構成することを考える．

いま，$G_1, G_2, \cdots, G_n$ を与えられた群とするとき，

$$G = \{(a_1, a_2, \cdots\cdots, a_n) | a_i \in G_i, i = 1, \cdots\cdots, n\}$$

とおく．G で，

$$(a_1, a_2, \cdots\cdots, a_n)(b_1, b_2, \cdots\cdots, b_n) = (a_1b_1, a_2b_2, \cdots\cdots, a_nb_n)$$

と乗法を定義すれば，G は群をつくる．実際，e_i を G_i の単位元とすれば，$e=(e_1, e_2, \cdots\cdots, e_n)$ は G の単位元であり，$(a_1, a_2, \cdots\cdots, a_n)^{-1}=(a_1^{-1}, a_2^{-1}, \cdots\cdots, a_n^{-1})$ である．この群 G を$G_1, G_2, \cdots\cdots, G_n$ の**直積**といって，$G=G_1\otimes G_2\otimes\cdots\cdots\otimes G_n$ で表す．

定義から，すぐわかるように，

$$G_1 \otimes G_2 \cong G_2 \otimes G_1$$

$$(G_1 \otimes G_2) \otimes G_3 \cong G_1 \otimes (G_2 \otimes G_3) \cong G_1 \otimes G_2 \otimes G_3$$

$G_i\cong G_i'$　$i=1, 2, \cdots\cdots, n$ ならば，

$$G_1 \otimes G_2 \otimes \cdots\cdots \otimes G_n \cong G_1' \otimes G_2' \otimes \cdots\cdots \otimes G_n'$$

$G=G_1\otimes G_2\otimes\cdots\cdots\otimes G_n$, $H=H_1\otimes H_2\otimes\cdots\cdots\otimes H_m$ ならば，

$$G \otimes H \cong G_1 \otimes \cdots\cdots \otimes G_n \otimes H_1 \otimes \cdots\cdots \otimes H_m$$

$G=G_1\otimes G_2\otimes\cdots\cdots\otimes G_n$ で，各 G_i が有限群ならば，

$$|G| = |G_1||G_2|\cdots\cdots|G_n|$$

例題 1. $G=G_1\otimes G_2\otimes\cdots\cdots\otimes G_n$ とし，N_i を G_i の正規部分群とすれば，$N=N_1\otimes N_2\otimes\cdots\cdots\otimes N_n$ は G の正規部分群であり，

$$G/N\cong G_1/N_1\otimes G_2/N_2\otimes\cdots\cdots\otimes G_n/N_n$$

証明 G_i から G_i/N_i への自然な準同型を f_i とし，

$$f(a_1, a_2, \cdots\cdots, a_n) = (f_1(a_1), f_2(a_2), \cdots\cdots, f_n(a_n))$$

とすれば，f は G から $G_1/N_1\otimes\cdots\cdots\otimes G_n/N_n$ の上への準同型である．$\mathrm{Ker}\,f=\{(a_1, \cdots\cdots, a_n) | 各\ f_i(a_i)=a_iN_i=N_i\}$ で，$a_iN_i=N_i$ となるのは $a_i\in N_i$ のとき，またそのときに限るから，$\mathrm{Ker}\,f=N$. ゆえに，準同型定理によって求める同型が得られる．

注 整数論における連立合同式に関する定理から，つぎの定理がみちびかれる．

[定理] $m\geqq 2$ を整数とし，$m=p_1^{e_1}p_2^{e_2}\cdots\cdots p_r^{e_r}$ を素因数分解とすれば，m を法とする既約剰余類群

$$\boldsymbol{Z}^*_m\cong \boldsymbol{Z}^*_{p_1^{e_1}}\otimes \boldsymbol{Z}^*_{p_2^{e_2}}\otimes\cdots\cdots \boldsymbol{Z}^*_{p_r^{e_r}}$$

この同型対応は，m に素な整数 a に対して，$a_i\equiv a(\mathrm{mod}\,p_i^{e_i})$ となる整数 a_i が $p_i^{e_i}$ を法として唯一つ定まるから，

a の法 m の剰余類

$\longmapsto$(a_1 の法 $p_1^{e_1}$ の剰余類，……，a_r の法 $p_r^{e_r}$ の剰余類)

によって与えられる．詳しくは，巻末文献〔23〕参照．

4-1-2　部分群の直積・群の直積分解

[定義]　$H_1, H_2, \cdots\cdots, H_n$ が群 G の部分群で，

(1) $i\neq j$ ならば $a_ia_j=a_ja_i$　$\forall a_i\in H_i,\ \forall a_j\in H_j$

(2) 積 $H_1H_2\cdots\cdots H_n$ の任意の元 a は，

$$a = a_1a_2\cdots\cdots a_n,\quad 各\ a_i\in H_i$$

と唯一通りに表せるとき，積 $H=H_1H_2\cdots\cdots H_n$ を，これら**部分群の直積**であるという．

$H_iH_j=H_jH_i$ であるから，H は G の部分群であり，H の元の積は $(a_1\ \cdots\cdots\ a_n)(b_1\ \cdots\cdots\ b_n)=(a_1b_1)\cdots\cdots(a_nb_n)$ となる．

[定義]　$G_1, G_2, \cdots\cdots, G_n$ は群 G の部分群で，

(1)　$i \neq j$ ならば，　$a_i a_j = a_j a_i \quad \forall a_i \in G_i,\ \forall a_j \in G_j$

(2)　G の任意の元 a は，

$$a = a_1 a_2 \cdots\cdots a_n, \qquad 各\ a_i \in G_i$$

と唯一通りに表されるとき，つまり G は $G_1, G_2, \cdots\cdots, G_n$ の直積であるとき，G は $G_1, G_2, \cdots\cdots, G_n$ の **直積に分解される**（**直積である**）といい，各 G_i をその **直積因子** という．

いま，群 G が与えられた群の直積 $G_1 \otimes G_2 \otimes \cdots\cdots \otimes G_n$ のとき，

$$G_i^* = \{a_i^* = (e_1, \cdots\cdots, e_{i-1}, a_i, e_{i+1}, \cdots\cdots e_n)\}$$

とすると，G_i^* は G_i と同型な G の部分群である．$i \neq j$ ならば，G_i^* の元 a_i^* と G_j^* の元 a_j^* は可換であり，G の任意元 $(a_1, a_2, \cdots\cdots, a_n)$ は

$$(a_1, a_2, \cdots\cdots, a_n) = a_1^* a_2^* \cdots\cdots a_n^*, \qquad 各\ a_i^* \in G_i^*$$

と唯一通りに表せる．したがって，G は部分群 $G_1^*, G_2^*, \cdots\cdots, G_n^*$ の直積である．

逆に，群 G が部分群 $G_1, G_2, \cdots\cdots, G_n$ の直積であるとき，

$$対応\ a_1 a_2 \cdots\cdots a_n \longrightarrow (a_1, a_2, \cdots\cdots, a_n)$$

によって，G は直積 $G_1 \otimes G_2 \otimes \cdots\cdots \otimes G_n$ と同型である．

そこで，群 G が部分群 $G_1, G_2, \cdots\cdots, G_n$ の直積のときにも，

$$G = G_1 \otimes G_2 \otimes \cdots\cdots \otimes G_n$$

と書くことにする．

群 G の部分群 $H_1, H_2, \cdots\cdots, H_n$ の直積 H も，各 H_i が H の部分群であるから，$H = H_1 \otimes H_2 \otimes \cdots\cdots \otimes H_n$ と表す．

部分群の直積について，つぎのことが成り立つ．

(1)　群 G が部分群 $G_1, G_2, \cdots\cdots, G_n$ の直積のとき各 $G_i \lhd G$．なぜなら，G の任意元 a は，

$$a = a_i b_i, \qquad a_i \in G_i, \qquad b_i \in G_1 \cdots\cdots G_{i-1} G_{i+1} \cdots\cdots G_n$$

と表され，b_i は G_i の元と可換であるから，

$$a G_i a^{-1} = a_i b_i G_i b_i^{-1} a_i^{-1} = a_i G_i a_i^{-1} = G_i$$

(2)　$H=H_1\otimes\cdots\cdots\otimes H_n$ も $K=K_1\otimes\cdots\cdots\otimes K_m$ も部分群の直積で，積 HK も直積ならば，

$$H\otimes K=H_1\otimes\cdots\cdots\otimes H_n\otimes K_1\otimes\cdots\cdots\otimes K_m$$

(3)　部分群 $H_1, H_2, \cdots\cdots H_n$ の積が直積ならば，$H_1, H_2, \cdots\cdots, H_r (r<n)$ の積も直積である．

(4)　部分群 $H_1, H_2, \cdots\cdots, H_n$ の積が直積ならば，r 個の直積 $H_1\otimes\cdots\cdots\otimes H_r$ と $n-r$ 個の直積 $H_{r+1}\otimes\cdots\cdots\otimes H_n$ の積も直積であり，

$$H_1\otimes H_2\otimes\cdots\cdots\otimes H_n=(H_1\otimes\cdots\cdots\otimes H_r)\otimes(H_{r+1}\otimes\cdots\cdots\otimes H_n)$$

(5)　$H=H_1\otimes\cdots\cdots\otimes H_n$ が直積で，$p_1, p_2, \cdots\cdots, p_n$ が $1, 2, \cdots\cdots, n$ の順列ならば，

$$H=H_{p_1}\otimes H_{p_2}\otimes\cdots\cdots\otimes H_{p_n}$$

(6)　$H=H_1\otimes\cdots\cdots\otimes H_n$ が直積で，$H_1', H_2', \cdots\cdots, H_n'$ がそれぞれ $H_1, H_2, \cdots\cdots, H_n$ の部分群ならば，

$$H_1'H_2'\cdots\cdots H_n'=H_1'\otimes H_2'\otimes\cdots\cdots\otimes H_n'$$

例題 1.　H_1, H_2, K は群 G の部分群で，積 $H_1H_2=H_1\otimes H_2$ で，$K\supset H_1$ とすると，$(H_1\otimes H_2)\cap K=H_1\otimes(H_2\cap K)$

証明　$(H_1\otimes H_2)\cap K\ni a=bc, b\in H_1, c\in H_2$ であるから，$c=b^{-1}a, b^{-1}\in H_1\subset K, a\in K$．したがって，$c\in H_2\cap K$ となり，$a\in H_1(H_2\cap K)$．ゆえに，$(H_1\otimes H_2)\cap K\subset H_1(H_2\cap K)$．

逆に $H_1(H_2\cap K)\ni bc, b\in H_1, c\in H_2\cap K$，とすれば，$c\in H_2$ であるから，$bc\in H_1H_2=H_1\otimes H_2$．また，$b\in H_1\subset K$，$c\in K$ であるから，$bc\in K$．したがって，$bc\in(H_1\otimes H_2)\cap K$．ゆえに，$(H_1\otimes H_2)\cap K\supset H_1(H_2\cap K)$ となる．したがって，$(H_1\otimes H_2)\cap K=H_1(H_2\cap K)$．つぎに，$H_2\cap K\subset H_2$ であるから，$H_1(H_2\cap K)=H_1\otimes(H_2\cap K)$ となる．

例題 2.　H, K を群 G の部分群とするとき，つぎの3条件は同値である．

(1)　HK の元は $hk, h\in H, k\in K$，の形に唯一通りに書ける

(2)　$hk=e, h\in H, k\in K$，ならば，$h=k=e$

(3)　$H\cap K=\{e\}$

証明 (1) ⟹ (2)　$hk=ee$ であるから，$h=e,\ k=e$.

(2) ⟹ (3)　$c\in H\cap K$ とすると $cc^{-1}=e$. ここで，$c\in H\cap K\subset H,\ c^{-1}\in H\cap K\subset K$, ゆえに $c=c^{-1}=e$, したがって $H\cap K=\{e\}$.

(3) ⟹ (1)　$HK\ni x=hk=h'k'$, $h,\ h'\in H$, $k,\ k'\in K$ とすれば，$h'^{-1}h=k'k^{-1}\in H\cap K=\{e\}$. ゆえに，$h'^{-1}h=k'k^{-1}=e$, $h=h'$, $k=k'$ となる.

例題 3.　$H,\ K$ が群 G の正規部分群で，$H\cap K=\{e\}$ ならば，

$$hk=kh \quad \forall h\in H,\ \forall k\in K$$

証明　$hkh^{-1}\in K,\ k^{-1}\in K$ であるから，$hkh^{-1}k^{-1}\in K$. 一方，$kh^{-1}k^{-1}\in H,\ h\in H$ であるから，$hkh^{-1}k^{-1}\in H$. したがって，$hkh^{-1}k^{-1}\subset H\cap K=\{e\}$，$hkh^{-1}k^{-1}=e$. ゆえに，$hk=kh$.

例題 4.　$H,\ K$ が群 G の正規部分群のとき，つぎの 4 条件は同値である.

(1)　積 $HK=H\otimes K$

(2)　HK の元は $hk,\ h\in H,\ k\in K$, の形に唯一通りに表せる

(3)　$hk=e,\ h\in H,\ k\in K$ ならば，$h=k=e$

(4)　$H\cap K=\{e\}$

証明　(1) ⟹ (2) は直積の定義より明らかであり，(2) ⟹ (3) ⟹ (4) は例題 2. (4) を仮定すれば，例題 3 より $hk=kh,\ \forall h\in H,\ \forall k\in K$ であり，また例題 2 から (2) が成り立つから，直積の定義によって $HK=H\otimes K$ となって，(1) が成り立つ.

以上から

［定理 1］　群 G が部分群 $G_1,\ G_2$ の直積であるための必要十分条件はつぎの 3 条件が成り立つことである.

(1)　$G_1,\ G_2$ は G の正規部分群である

(2)　G の任意の元は $ab,\ a\in G_1,\ b\in G_2$, の形に表せる

(3)　$G_1\cap G_2=\{e\}$

［証明］　$G=G_1\otimes G_2$ であれば，もちろん $G=G_1G_2$ ゆえ，(2) は明らかである. 先に述べたように各 $G_i\triangleleft G$ であるから (1) が，また例題 4 より (3) も成り立つ.

逆に (1), (2), (3) が成り立てば，(1), (3) から，$G_1G_2=G_1\otimes G_2$ となり（例題 4），(2) から $G=G_1G_2$ であるから，$G=G_1\otimes G_2$ となる.

また，例題4の(2)と(4)が同値であることから，

[定理 2]　群 G が部分群 G_1, G_2 の直積であるための必要十分条件はつぎの3条件が成り立つことである．

(1) G_1, G_2 が G の正規部分群である．

(2) G の任意の元は ab, $a \in G_1$, $b \in G_2$, の形に表せる．

(3) G の任意の元は ab, $a \in G_1$, $b \in G_2$, の形に唯一通りに表せる．

例 1.　クラインの4元群 $V=\{e, a, b, c\}$, $ab=ba=c$, $a^2=b^2=e$, において，$\langle a \rangle$, $\langle b \rangle \lhd V$, $c=ab$ であるから $V=\langle a \rangle \langle b \rangle$. また $\langle a \rangle \cap \langle b \rangle = \{e\}$ であるから，$V=\langle a \rangle \otimes \langle b \rangle$.

例題 5.　法 $2^m (m \geqq 3)$ の既約剰余類のつくる乗法群 G は，位数2の巡回群 $\langle C(-1) \rangle$ と位数 2^{m-2} の巡回群 $\langle C(-5) \rangle$ の直積である．

証明　$|G|=\varphi(2^m)=2^{m-1}$ である．$H=\langle C(-1) \rangle$ は，位数2の巡回群である．$K=\langle C(-5) \rangle$ の位数が 2^{m-2} であることをいう．そのために，$5^{2^{\nu-2}}=1+k_\nu 2^\nu$ (k_ν は奇数), $\nu \geqq 2$, が成り立つことを示す．この式は，$\nu=2$ のとき $5^1=1+1 \cdot 2^2$ であるから正しい．いま $\nu (\nu \geqq 2)$ について，この式が成り立つとすれば，$5^{2^{(\nu+1)-2}}=(1+k_\nu 2^\nu)^2=1+k_\nu 2^{\nu+1}+k_\nu^2 2^{2\nu}=1+(k_\nu+2^{\nu-1}k_\nu^2)2^{\nu+1}=1+k_{\nu+1}2^{\nu+1}$ であって，ここで $k_{\nu+1}=k_\nu+2^{\nu-1}k_\nu^2$ は奇数である．したがって，

$$5^{2^{m-2}} = 1 + k_m 2^m, \qquad 5^{2^{m-3}} = 1 + k_{m-1} 2^{m-1}$$

$$5^{2^{m-2}} \equiv 1 \pmod{2^m}, \quad 5^{2^{m-3}} \not\equiv 1 \pmod{2^m}$$

であるから，$C(5)$ の位数は 2^{m-2} である．

さて，$H \cap K=\{C(1)\}$ である．もしもそうでなければ，

$$C(5)^\lambda = C(-1), \qquad 5^\lambda \equiv -1 \pmod{2^m}$$

となり，$(1+4)^\lambda \equiv -1 \pmod 4$, $1 \equiv -1 \pmod 4$ となって，矛盾する．したがって，例題4より $HK=H \otimes K$ となるが，$|H \otimes K|=2 \times 2^{m-2}=2^{m-1}$ であるから，$H \otimes K=G$.

[定理 3]　H, K は群 G の位数が有限な正規部分群で，位数が互いに素ならば，積 HK は直積である．一般に，G の正規部分群 $H_1, H_2, \cdots\cdots, H_r$ が有限群で，どの2つも位数が互いに素ならば，積 $H_1 \cdots\cdots H_r$ は直積である．

[証明]　$|H|=m$, $|K|=n$ とすれば，$H \cap K$ の位数は，m, n の公約数であるから

1で，$H\cap K=\{e\}$．したがって，例題4より $HK=H\otimes K$．一般の場合は r に関する帰納法で証明する．帰納法の仮定により，$K=H_2\cdots\cdots H_r$ は直積であり，$K\lhd G$．$|K|=n_2\cdots\cdots n_r$ と $|H_1|=n_1$ とは互いに素であるから，$H_1K=H_1\otimes K$．したがって，$H_1H_2\cdots\cdots H_r=H_1\otimes H_2\otimes\cdots\cdots\otimes H_r$．

例題 6． $m_1, m_2, \cdots\cdots, m_r$ はどの2つも互いに素な自然数で，G は位数 $m_1m_2\cdots\cdots m_r$ の巡回群とする．G_i を G の位数 m_i の（唯一つしかない）部分群とすれば，$G=G_1\otimes G_2\otimes\cdots\cdots\otimes G_r$．

証明　$G'=G_1G_2\cdots\cdots G_r$ は直積であるが，$|G'|=|G|$ であるから，$G=G'$．

いま，G が位数 n の巡回群のとき，$n=p_1^{e_1}p_2^{e_2}\cdots\cdots p_r^{e_r}$ を素因数分解とすれば，G は位数がそれぞれ $p_1^{e_1}$, $p_2^{e_2}$, $\cdots\cdots$, $p_r^{e_r}$ の r 個の巡回群の直積に，一意的に分解される．

さて，先の定理1を一般化してみよう．まず，例題2，4を一般化してみる．

例題 7． $H_1, H_2, \cdots\cdots, H_n$ を群 G の部分群とし，任意の i, j に対して $H_iH_j=H_jH_i$ となるとき，つぎの3条件は互いに同値である．

(1)　積 $H_1H_2\cdots\cdots H_n$ の元は $a_1a_2\cdots\cdots a_n$，各 $a_i\in H_i$，の形に唯一通りに表される．

(2)　$a_1a_2\cdots\cdots a_n=e$（各 $a_i\in H_i$）ならば $\forall a_i=e$．

(3)　$H_1H_2\cdots\cdots H_{i-1}\cap H_i=\{e\}$，　$i=2, 3, \cdots\cdots, n$．

証明　(1) ⟹ (2)　　$a_1a_2\cdots\cdots a_n=ee\cdots\cdots e$ であるから，$a_1=e, a_2=e, \cdots\cdots, a_n=e$．

(2) ⟹ (3)　　$c\in H_1H_2\cdots\cdots H_{i-1}\cap H_i$ とすると $c=a_1a_2\cdots\cdots a_{i-1}$，各 $a_j\in H_j$, $j=1, 2, \cdots\cdots, i-1$．また，$c\in H_i$ より $c^{-1}\in H_i$ であるから，$c^{-1}=a_i\in H_i$．$a_{i+1}=\cdots\cdots=a_n=e$ とすると $a_1a_2\cdots\cdots a_n=a_1a_2\cdots\cdots a_{i-1}a_i=e$．したがって $a_1=\cdots\cdots a_n=e$．とくに，$a_i=c^{-1}=e$, $c=e$ であるから，$H_1H_2\cdots\cdots H_{i-1}\cap H_i=\{e\}$．

(3) ⟹ (1)　　n に関する帰納法による．$n=2$ のときは例題2により正しい．帰納法の仮定により $K=H_1H_2\cdots\cdots H_{n-1}$ の各元は $a_1a_2\cdots\cdots a_{n-1}$，各 $a_i\in H_i$, $1\leqq i\leqq n-1$，と唯一通りに表せる．K は，$H_iH_j=H_jH_i$ より，G の部分群であり，$K\cap H_n=\{e\}$ であるから，例題2によって KH_n の元は ba_n, $b\in K$, $a_n\in H_n$，の形に唯一通りに表されるから，$H_1H_2\cdots\cdots H_n$ の元は $a_1a_2\cdots\cdots a_n$，各 $a_i\in H_i$, $1\leqq i\leqq n$，の形に唯一通りに表せる．

例題 8.　$H_1, H_2, \cdots\cdots, H_n$ が群 G の正規部分群のとき，つぎの4条件は互いに同値である．

(1)　積 $H_1H_2\cdots\cdots H_n=H_1\otimes H_2\otimes\cdots\cdots\otimes H_n$.

(2)　$H_1H_2\cdots\cdots H_n$ の元が $a_1a_2\cdots\cdots a_n$,　各 $a_i\in H_i$, の形に唯一通りに表せる．

(3)　$a_1a_2\cdots\cdots a_n=e$（各 $a_i\in H_i$）ならば，$\forall a_i=e$.

(4)　$H_1H_2\cdots\cdots H_{i-1}\cap H_i=\{e\}$,　$i=2, 3, \cdots\cdots, n$.

証明　(1) $\Longrightarrow$ (2) は直積の定義より明らかであり，(2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) は例題7である．(4) を仮定すると，例題7によって，(2) が成り立つから，$H_1H_2\cdots\cdots H_n$ の元は，$a_1a_2\cdots\cdots a_n$,　各 $a_i\in H_i$, の形に唯一通りに書ける．いま，$i\neq j$ で，$i<j$ ならば $H_i\subset H_1\cdots\cdots H_{j-1}$ であるから，$H_i\cap H_j=\{e\}$ となる．H_i, H_j ともに G の正規部分群であるから，例題3によって，H_i の元と H_j の元は可換である．ゆえに，直積の定義より積 $H_1H_2\cdots\cdots H_n$ は直積である．

以上から，定理1，2の一般化として，つぎの定理がみちびかれる．

[定理 4]　群 G が部分群 $G_1, G_2, \cdots\cdots, G_n$ の直積であるための必要十分条件は，つぎの3条件が成り立つことである．

(1)　$G_1, G_2, \cdots\cdots, G_n$ は G の正規部分群である．

(2)　$G=G_1G_2\cdots\cdots G_n$

(3)　$G_1G_2\cdots\cdots G_{i-1}\cap G_i=\{e\}$,　$i=2, 3, \cdots\cdots, n$

[定理 5]　群 G が部分群 $G_1, G_2, \cdots\cdots, G_n$ の直積であるための必要十分条件は，つぎの3条件が成り立つことである．

(1)　$G_1, G_2, \cdots\cdots, G_n$ は G の正規部分群である．

(2)　$G=G_1G_2\cdots\cdots G_n$

(3)　G の任意の元は $a_1a_2\cdots\cdots a_n$,　各 $a_i\in G_i$, と唯一通りに表される．

注　加法群 $H_1, H_2, \cdots\cdots, H_n$ の直積 H を**普通直和**といい，記号で

$$H=H_1\oplus H_2\oplus\cdots\cdots\oplus H_n$$

と書く．すなわち，$H=\{(a_1, a_2, \cdots\cdots, a_n)\,|\,\text{各 } a_i\in H_i\}$ であって，H での加法は

$$(a_1, a_2, \cdots\cdots, a_n)+(b_1, b_2, \cdots\cdots, b_n)=(a_1+b_1, a_2+b_2, \cdots\cdots, a_n+b_n)$$

で定義される.

また，加法群 G が部分群 $G_1, G_2, \cdots\cdots, G_n$ の直和であるための条件は G の任意の元 a が $a=a_1+a_2+\cdots\cdots+a_n,\ a_i\in G_i,$ と唯一通りに表されることである.

4-2 アーベル群

4-2-1 自由アーベル群

いくつかの無限巡回群 $\langle u_1\rangle, \langle u_2\rangle, \cdots\cdots, \langle u_r\rangle$ の直積

$$F=\langle u_1\rangle\otimes\langle u_2\rangle\otimes\cdots\cdots\otimes\langle u_r\rangle$$

を**自由アーベル群**といい，直積因子の生成元 $u_1, u_2, \cdots\cdots, u_r$ をその**自由生成元**または**底**という. 自由アーベル群 F の元は

$$u=u_1^{n_1}u_2^{n_2}\cdots\cdots u_r^{n_r},\quad 各\ n_i\in \boldsymbol{Z},$$

という形に唯一通りに表される.

上記 $\langle u_i\rangle$ が加法群であるときは直積の代りに直和

$$M=\langle u_1\rangle\oplus\langle u_2\rangle\oplus\cdots\cdots\oplus\langle u_r\rangle$$

を考えて，これを $u_1, u_2, \cdots\cdots, u_r$ を底とする（または，$u_1, u_2, \cdots\cdots, u_r$ から生成された）**自由加群**という. このとき M の元は,

$$u=n_1u_1+n_2u_2+\cdots\cdots+n_ru_r,\qquad 各\ n_i\in \boldsymbol{Z},$$

という形に唯一通りに表される.

すぐあとで示すように，自由アーベル群の底のとり方は1通りに限らない. しかし，底に属する元の個数はつぎの定理の示すように一定である.

[定理 6] 自由アーベル群の底に属する元の個数は，底のとり方に無関係に一定である. 底に属する元の個数を自由アーベル群の**階数**という.

[証明] $F=\langle u_1\rangle\otimes\cdots\cdots\otimes\langle u_r\rangle=\langle v_1\rangle\otimes\cdots\cdots\otimes\langle v_s\rangle$ とする. n を1より大きい自然数として，$F^n=\{x^n|x\in F\}$ とおくと $F^n=\langle u_1^n\rangle\otimes\cdots\cdots\otimes\langle u_r^n\rangle=\langle v_1^n\rangle\otimes\cdots\cdots\otimes\langle v_s^n\rangle$, 各 $\langle u_i^n\rangle\lhd\langle u_i\rangle$, $\langle v_j^n\rangle\lhd\langle v_j\rangle$ であるから,

$$F/F^n=(\langle u_1\rangle/\langle u_1^n\rangle)\otimes\cdots\cdots\otimes(\langle u_r\rangle/\langle u_r^n\rangle)$$

$$=(\langle v_1\rangle/\langle v_1{}^n\rangle)\otimes\cdots\cdots\otimes(\langle v_s\rangle/\langle v_s{}^n\rangle)$$

さて，$\langle u_i\rangle/\langle u_i{}^n\rangle$，$\langle v_j\rangle/\langle v_j{}^n\rangle$ は位数 n の巡回群であるから，F/F^n の2通りの直積による表現での位数を比較して $n^r=n^s$．したがって $r=s$．

例題 1． 自由加群 M の底 $u_1, u_2, \cdots\cdots, u_n$ が M に属する n 個の元 $v_1, v_2, \cdots\cdots, v_n$ によって，

$$u_i=\sum_{k=1}^{n} a_{ik}v_k, \qquad 各\ a_{ik}\in \boldsymbol{Z},$$

と表されるならば，$v_1, v_2, \cdots\cdots, v_n$ も M の底である．

証明　M は加群として $v_1, v_2, \cdots\cdots, v_n$ から生成される．$N=\langle x_1\rangle\oplus\cdots\cdots\oplus\langle x_n\rangle$ を自由加群とすると，対応 $f(a_1x_1+\cdots\cdots+a_nx_n)=a_1v_1+\cdots\cdots+a_nv_n$ によって，N は M の上に準同型にうつされる．f の核に属する任意の元を w とする．$f(y_i)=u_i$，$i=1, 2, \cdots\cdots, n$，となる N の元 $y_1, y_2, \cdots\cdots, y_n$ をとる．$w=\sum_{j=1}^{n} a_jx_j$，$y_i=\sum_{j=1}^{n} b_{ij}x_j$，$a_j, b_{ij}\in\boldsymbol{Z}$，とすると，整数を成分とする $n+1$ 個の n 次元数ベクトル $\boldsymbol{a}=(a_j)$，$\boldsymbol{b}_i=(b_{ij})$，$i=1, 2, \cdots\cdots, n$ は有理数体 $\boldsymbol{Q}$ 上1次従属であるから，$c\boldsymbol{a}+\sum_{i=1}^{n} c_i\boldsymbol{b}_i=\boldsymbol{0}$ となる整数 $c, c_1, c_2, \cdots\cdots, c_n$ が存在する．ただし，これら $n+1$ 個の整数のうち少なくとも1つは0でない．したがって，

$$cw+c_1y_1+c_2y_2+\cdots\cdots+c_ny_n=0$$

さて，$f(w)=0$, $f(y_i)=u_i$ であるから，

$$\begin{aligned}&f(cw+c_1y_1+\cdots\cdots+c_ny_n)\\&=c_1u_1+c_2u_2+\cdots\cdots+c_nu_n=0\end{aligned}$$

となり，$c_1=c_2=\cdots\cdots=c_n=0$ となる．ゆえに $c\neq 0$ で，$cw=0$ より，$w=0$ となる．すなわち，$\mathrm{Ker}\,f=\{0\}$ で，f は N から M への同型である．ゆえに，$\sum a_iv_i=0$ なら $\sum a_ix_i=0$ であり，したがって，各 $a_i=0$．すなわち，M の元は $\sum_{i=1}^{n} n_iv_i$，各 $n_i\in\boldsymbol{Z}$，と書けるだけでなく，このような表し方も1通りである．ゆえに，$v_1, v_2, \cdots\cdots, v_n$ も M の底である．

例題 2． 自由加群 M の1つの底を $u_1, u_2, \cdots\cdots, u_n$ とし，整数を成分にもつ n 次正方行列 $A=(a_{ij})$ が，整数の範囲で逆行列をもつならば，

$$v_i=\sum_{j=1}^{n} a_{ij}u_j,\ \ i=1, 2, \cdots\cdots, n$$

は M の底である．逆に M の底はすべてこのようにして得られる．

証明 A が逆行列 $A^{-1}=(b_{ij})$, $b_{ij}\in\boldsymbol{Z}$, をもてば,

$$u_i=\sum_{j=1}^{n}b_{ij}v_j,\quad i=1,2,\cdots\cdots,n,\quad 各\ b_{ij}\in\boldsymbol{Z},$$

であるから，例題1より $v_1, v_2, \cdots\cdots, v_n$ は M の底となる．つぎに，$v_1, v_2, \cdots\cdots, v_n$ を M の任意の底とすれば,

$$v_i=\sum_{j=1}^{n}a_{ij}u_j,\quad u_i=\sum_{j=1}^{n}b_{ij}v_j,\quad i=1,2,\cdots\cdots,n$$

ここで，各 $a_{ij}\in\boldsymbol{Z}$, 各 $b_{ij}\in\boldsymbol{Z}$, となるから,

$$(a_{ij})(b_{ij})=E\quad(n\ 次単位行列)$$

となり，(b_{ij}) は (a_{ij}) の逆行列である．

注 整数を成分とする n 次の行列 A が整数の範囲に逆行列をもつために必要十分条件は A の行列式 $|A|=\pm1$ である．このような行列を**ユニモヂュラー行列**という．

[定理 7] F は階数 r の自由アーベル群とする．F の任意の部分群 H はまた自由アーベル群で，その階数を s とすれば $s\leqq r$ である．また，F の底 $u_1, u_2, \cdots\cdots, u_r$ を適当にとれば,

$$H=\langle u_1^{e_1}\rangle\otimes\cdots\cdots\otimes\langle u_s^{e_s}\rangle$$

とできる．さらに，$e_1, e_2, \cdots\cdots, e_s$ は正の整数で

$$e_1|e_2,\quad e_2|e_3,\quad\cdots\cdots,\quad e_{s-1}|e_s$$

となるようにできる．

[証明] $r=1$ のときは $F=\langle u_1\rangle$ で，無限巡回群 F の部分群 H は無限巡回群で，$H=\langle u_1^{e_1}\rangle$ となる．そこで，階数が $r-1$ 以下のとき定理は正しいとして，r に関する帰納法で証明する．

はじめに，F の1つの底の H に関する高さという考えを説明する．$F=\langle x_1\rangle\otimes\cdots\cdots\otimes\langle x_r\rangle$ のとき，H の元 $w=x_1^{a_1}x_2^{a_2}\cdots\cdots x_r^{a_r}$ と唯一通りに表されるが，w が H の中を動くとき，0でない $|a_i|$ の最小値を，底 $x_1, x_2, \cdots\cdots, x_r$ の H に関する高さという．F の底をいろいろ変えると，高さは変わるかもしれないが，適当な底を選んで，高さが最小になるものを改めて $x_1, x_2, \cdots\cdots, x_r$ とし，その高さを h とする．このとき，H の中に元 $w=x_1^{a_1}\cdots\cdots x_r^{a_r}$ があって，ある $|a_i|=h$ となっている．必要ならば番号を付け変えて，$|a_1|=h$ と仮定してよい．また，$a_1<0$ であれば，$w^{-1}\in H$ を考え

ればよいから $a_1=h$ としてよい．さて，このとき $a_1|a_j,\ j=2,\ \cdots\cdots,\ r$ である．実際，$a_j=a_1q_j+r_j,\ 0\leqq r_j<a_1=h$，とし，ある $r_k\neq 0$ ならば，$u_1=x_1x_2^{q_2}\cdots\cdots x_r^{q_r}$ とおくとき，$u_1^{a_1}x_2^{r_2}\cdots\cdots x_r^{r_r}=w\in H$ であり，例題1から，$u_1,\ x_2,\ \cdots\cdots,\ x_r$ は F の底であり，この底の H に関する高さは r_k 以下となり，h の最小性に反する．したがって，$r_k=0,\ a_k=a_1q_k$，

$$\begin{cases} F=\langle u_1\rangle\otimes\langle x_2\rangle\otimes\cdots\cdots\otimes\langle x_r\rangle \\ w=u_1^{a_1}\in H \end{cases}$$

つぎに，H の任意の元を $v=u_1^{b_1}x_2^{b_2}\cdots\cdots x_r^{b_r}$ とし，$b_1=a_1q+s,\ 0\leqq s<a_1=h$ とすれば，$H\ni vw^{-q}=u_1^{s}x_2^{b_2}\cdots\cdots x_r^{b_r}$ で，$s\neq 0$ ならば，h の最小性に反するから，$s=0,\ v=(u_1^{a_1})^qx_2^{b_2}\cdots\cdots x_r^{b_r}$．さて $x_2^{b_2}\cdots\cdots x_r^{b_r}=v(u_1^{a_1})^{-q}\in H$ であるから，$H_1=H\cap\langle x_2,\ \cdots\cdots,\ x_r\rangle$ とおくと，$x_2^{b_2}\cdots\cdots x_r^{b_r}\in H_1$ であり，$v\in\langle u_1^{a_1}\rangle H_1$．また，$\langle u_1^{a_1}\rangle\cap H_1\ni w'=(u_1^{a_1})^n=x_2^{c_2}\cdots\cdots x_r^{c_r},\ (u_1^{a_1})^n=x_1^nx_2^{nq_2}\cdots\cdots x_r^{nq_r}$ であるから，$n=0,\ w'=e$ となるので，$\langle u_1^{a_1}\rangle\cap H_1=\{e\}$．ゆえに $H=\langle u_1^{a_1}\rangle\otimes H_1$．

さて，自由アーベル群 $F_1=\langle x_2\rangle\otimes\cdots\cdots\otimes\langle x_r\rangle$ とその部分群 H_1 に帰納法の仮定を適用して，F_1 の底 $u_2,\ u_3,\ \cdots\cdots,\ u_r$ を適当にとって，$H_1=\langle u_2^{a_2}\rangle\otimes\cdots\cdots\otimes\langle u_s^{a_s}\rangle$，ここで，各 a_i は正の整数であり，$a_2|a_3,\ a_3|a_4,\ \cdots\cdots,\ a_{s-1}|a_s$，とできる．このとき，つぎのようになっている．

$$F=\langle u_1\rangle\otimes F_1=\langle u_1\rangle\otimes\langle u_2\rangle\otimes\cdots\cdots\otimes\langle u_r\rangle$$
$$H=\langle u_1^{a_1}\rangle\otimes\langle u_2^{a_2}\rangle\otimes\cdots\cdots\otimes\langle u_s^{a_s}\rangle$$

最後に $a_1|a_2$ を示せば，定理は証明されたことになる．$a_2=a_1q+t,\ 0\leqq t<a_1=h$，とし，$t\neq 0$ とすれば，$H\ni u_1^{a_1}u_2^{a_2}=(u_1u_2^q)^{a_1}u_2^t$ で，$u_1u_2^q,\ u_2,\ \cdots\cdots,\ u_r$ は F の底で，この底の H に関する高さは t 以下で，h の最小性に反する．したがって，$t=0,\ a_1|a_2$ となる．

4-2-2　有限生成アーベル群

有限個の元から生成されたアーベル群を**有限生成アーベル群**という．位数が有限のアーベル群は，その元全体を生成元と考えてよいから，有限生成である．

[定理 8]　有限生成アーベル群は巡回群の直積である．

[証明]　G を $a_1,\ a_2,\ \cdots\cdots,\ a_r$ を生成元とするアーベル群とする．いま，$F=\langle x_1\rangle\otimes\langle x_2\rangle\otimes\cdots\cdots\otimes\langle x_r\rangle$ を $x_1,\ x_2,\ \cdots\cdots,\ x_r$ を生成元とする自由アーベル群とし，F

から G の上へのつぎのような写像 φ を考える：

$$\varphi: x_1^{n_1}x_2^{n_2}\cdots\cdots x_r^{n_r} \longmapsto a_1^{n_1}a_2^{n_2}\cdots\cdots a_r^{n_r}$$

φ は準同型であって，$H=\mathrm{Ker}\,\varphi$ とすれば，$F/H\cong G$．定理7によって，F の底を

$$F=\langle u_1\rangle\otimes\cdots\cdots\otimes\langle u_r\rangle$$

$$H=\langle u_1^{e_1}\rangle\otimes\cdots\cdots\otimes\langle u_s^{e_s}\rangle,\ e_i>0,\ e_1|e_2,\ \cdots\cdots,\ e_{s-1}|e_s$$

となるようにとっておくと，F/H はつぎのように直積に分解する：

$$F/H=(\langle u_1\rangle/\langle u_1^{e_1}\rangle)\otimes\cdots\cdots\otimes(\langle u_s\rangle/\langle u_s^{e_s}\rangle)\otimes\langle u_{s+1}\rangle\otimes\cdots\cdots\otimes\langle u_r\rangle$$

ここで，$\langle u_i\rangle/\langle u_i^{e_i}\rangle$ は位数が e_i の有限巡回群，$\langle u_{s+1}\rangle$，……，$\langle u_r\rangle$ は無限巡回群である．そこで，$\varphi(u_i)=b_i$ とすれば，

$$G=\langle b_1\rangle\otimes\cdots\cdots\otimes\langle b_s\rangle\otimes\langle b_{s+1}\rangle\otimes\cdots\cdots\otimes\langle b_r\rangle$$

となり，$1\leqq i\leqq s$ のとき $\langle b_i\rangle$ は位数 e_i の有限巡回群であって，$e_1|e_2$, $e_2|e_3$, ……, $e_{s-1}|e_s$，また，$\langle b_{s+1}\rangle$，……，$\langle b_r\rangle$ は無限巡回群である．

上の証明で，$e_1=e_2=\cdots\cdots=e_k=1$, $e_{k+1}>1$ であれば，$\langle b_1\rangle=\cdots\cdots=\langle b_k\rangle=\langle e\rangle$ であるから，これら k 個の直積因子は除いてよい．

上の結果から，つぎの定理の前半が得られる．

[定理 9]　有限生成アーベル群 G は，

$$G=\langle a_1\rangle\otimes\cdots\cdots\otimes\langle a_t\rangle\otimes\langle b_1\rangle\otimes\cdots\cdots\otimes\langle b_s\rangle$$

と巡回群の直積に分解される．ここで，$\langle a_i\rangle$ は位数 e_i の有限巡回群で，$e_1\geqq e_2\geqq\cdots\cdots\geqq e_t>1$，しかも，$e_i|e_{i-1}$, $2\leqq i\leqq t$．$\langle b_j\rangle$ は無限巡回群である．さらに，$\langle b_j\rangle$ には位数として0を考えることにすると，$(e_1, e_2, \cdots\cdots, e_t, 0, \cdots\cdots, 0)$ という位数の組は G によって一意的に定まる．

[証明]　最後の部分を証明すればよい．定理のような直積分解を，

$$G=\langle a_1'\rangle\otimes\cdots\cdots\otimes\langle a_{t'}'\rangle\otimes\langle b_1'\rangle\otimes\cdots\cdots\otimes\cdots\cdots\otimes\langle b_{s'}'\rangle$$

とし，$\langle a_i'\rangle$ の位数を e_i' とする．さて G の有限位数の元全体は1つの部分群 T をつくる．T を G の**振れの群**という．

$$T=\langle a_1\rangle\otimes\cdots\cdots\otimes\langle a_t\rangle,\ \text{また}\ T=\langle a_1'\rangle\otimes\cdots\cdots\otimes\langle a_{t'}'\rangle$$

$$\therefore\ G/T\cong\langle b_1\rangle\otimes\cdots\cdots\otimes\langle b_s\rangle,\quad \cong\langle b_1'\rangle\otimes\cdots\cdots\otimes\langle b_{s'}'\rangle$$

これら2つの直積はいずれも自由アーベル群であるから，$s=s'$．

つぎに T について，$t\neq t'$ ならば，小さい方に位数1の単位群をいくつかつけ加えて $t=t'$ としておく．$e_1=e_1'$, ……, $e_{\nu-1}=e'_{\nu-1}$, $e_\nu\neq e_\nu'$，たとえば，$e_\nu'>e_\nu$ ならば，

$e_t|e_\nu$, ……, $e_{\nu+1}|e_\nu$ であるから，

$$T^{e_\nu}=\langle a_1{}^{e_\nu}\rangle\otimes\cdots\cdots\otimes\langle a_{\nu-1}{}^{e_\nu}\rangle$$
$$=\langle a_1{}'^{e_\nu}\rangle\otimes\cdots\cdots\otimes\langle a'_{\nu-1}{}^{e_\nu}\rangle\otimes\langle a_\nu{}'^{e_\nu}\rangle\otimes\cdots\cdots\otimes\langle a_{t'}{}'^{e_\nu}\rangle$$

$\langle a_1{}^{e_\nu}\rangle$, ……, $\langle a_{\nu-1}{}^{e_\nu}\rangle$ の位数はそれぞれ $\langle a_1{}'^{e_\nu}\rangle$, ……, $\langle a'_{\nu-1}{}^{e_\nu}\rangle$ の位数に等しく，e_1/e_ν, ……, $e_{\nu-1}/e_\nu$ である．$e_\nu'>e_\nu$ であるから，$\langle a_\nu{}'^{e_\nu}\rangle\neq\{e\}$ であって，位数を比較して矛盾を得る．$e_\nu'<e_\nu$ であれば，$T^{e_\nu'}$ について，上と同様にして，矛盾を得る．よって，$e_i=e_i'$, $i=1, 2, \cdots\cdots, t$, である．

［定義］　有限生成アーベル群 G に対して，上記のようにして定まる一定な位数の組 $(e_1, e_2, \cdots\cdots, e_t, 0, \cdots\cdots, 0)$，ここで $e_i|e_{i-1}$, $i=2, \cdots\cdots, t$, を G の**不変系**という．たとえば，自由アーベル群の不変形は $(0, 0, \cdots\cdots, 0)$ であり，クラインの4元数の不変系は $(2, 2)$ である．また，定理9における $t+s$ 個の生成元の組 $a_1, a_2, \cdots\cdots, a_t, b_1, \cdots\cdots, b_s$ を G の**底**という．

G を位数 m の巡回群とする．p. 81 の例題 6 で述べたように，$m=m_1m_2\cdots\cdots m_r$，ここで，$(m_i, m_j)=1$, $i\neq j$, ならば，G は位数がそれぞれ $m_1, m_2, \cdots\cdots, m_r$ の r 個の巡回群の直積になる．とくに，m の素因数分解を $m=p_1{}^{n_1}p_2{}^{n_2}\cdots\cdots p_r{}^{n_r}$ とすれば，G は位数がそれぞれ $p_1{}^{n_1}, p_2{}^{n_2}, \cdots\cdots, p_r{}^{n_r}$ の r 個の巡回群の直積になる．

逆に，$\langle a\rangle$, $\langle b\rangle$ がそれぞれ位数 m, n の巡回部分群で，$(m, n)=1$ であれば，積 $\langle a\rangle\langle b\rangle$ は直積であり（p. 80，定理 3），ab の位数は mn であるから（p. 36，例題 1），$\langle a\rangle\otimes\langle b\rangle=\langle ab\rangle$ となる．一般に，$\langle a_i\rangle$ の位数が m_i で，$(m_i, m_j)=1$, $i\neq j$, ならば $\langle a_1\rangle\otimes\cdots\cdots\otimes\langle a_r\rangle=\langle c\rangle$，ここで $c=a_1a_2\cdots\cdots a_r$, となる．

例題 1.　有限生成アーベル群は，位数が素数巾の巡回群か，無限巡回群のとき，そのときに限って，2つ以上の真の部分群の直積に分解されない．

証明　$G=\langle a\rangle$ を位数が p^n の巡回群とする．$n=1$ のときは明らか．$n\geqq2$ とする．G の真の部分群 H, K はともに位数が p の巾の巡回群で，ともに位数 p の部分群を含む．G の位数 p の部分群は1つだけであるから，$H\cap K\neq\{e\}$．したがって，G は2つ以上の真の部分群の直積にはならない．また，$G=\langle a\rangle$ が無限巡回群のときは，

2つの部分群 $H=\langle a^n\rangle$ と $K=\langle a^m\rangle$ は元 a^{mn} を共通に含むから，$H\cap K\neq\{e\}$. したがって，G は2つ以上の真の部分群の直積にならない.

逆に有限生成アーベル群は巡回群の直積になるから，2つ以上の真の部分群の直積にならないためには，まず巡回群でなくてはならない. さらに無限巡回群か，または位数が素数の巾かでなければならない. もしもそうでなければ，2つ以上の真の巡回部分群の直積になるからである.

4-2-3 有限アーベル群

G を有限アーベル群とすれば，G は，たとえば，G の元全体を生成元にとればよいから，有限生成アーベル群であり，定理8から，

$$G = G_1 \otimes G_2 \otimes \cdots\cdots \otimes G_r$$

と巡回群の直積になり，$|G_i|=m_i$ とすれば，$|G| = m_1m_2\cdots\cdots m_r$

いま，$m_i=p_1^{r_1}p_2^{r_2}\cdots\cdots p_t^{r_t}$ を素因数分解とすれば，巡回群 G_i はさらに位数 $p_i^{r_i}$ の巡回群の直積に分解されるから，G は素数巾位数の巡回群の直積に分解される.

［定理 10］ G を有限アーベル群とし，$|G|=n$ を相異なる素数の巾の積に分解して $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_s^{\alpha_s}$ とすれば，G は位数が $p_i^{\alpha_i}$ の部分群 P_i をもつ. $P_i=\{x|x\in G,\ x^{p_i^{\alpha_i}}=e\}$ であって，G はこれら s 個の $P_1, P_2, \cdots\cdots, P_s$ の直積である.

［証明］ G は素数巾位数の巡回群の直積になるので，位数が p_i の巾である巡回群すべての直積を P_i とすると，明らかに $|P_i|=p_i^{\alpha_i}$ であり，$G=P_1\otimes P_2\otimes\cdots\cdots\otimes P_s$ である (p. 80，定理3).

ここで，つぎの補題を証明する.

［補題］ G_1, G_2 はそれぞれ位数 m, n のアーベル群で，$(m, n)=1$ とする. $G=G_1\otimes G_2$ とするとき

$$G_1 = \{x|x \in G,\ x^m = e\}, \qquad G_2 = \{x|x \in G,\ x^n = e\}$$

証明 G の元 x は $x=x_1x_2,\ x_i\in G_i,\ i=1, 2,$ と表される. $x^m=x_1{}^m x_2{}^m=e \Leftrightarrow x_1{}^m=e,\ x_2{}^m=e \Leftrightarrow x_2=e \Leftrightarrow x=x_1 \Leftrightarrow x\in G_1$ であるから，はじめの等式を得る. 後の等式も同様.

さて，この補題は2つ以上の，位数が互いに素であるアーベル群に対して一般化できる．したがって，$P_i=\{x|x\in G,\ x^{p_i^{\alpha_i}}=e\}$ となる．

さて，上記の P_i を巡回群の直積に分解して，

$$P_i=\langle a_{i1}\rangle\otimes\langle a_{i2}\rangle\otimes\cdots\cdots\otimes\langle a_{ir_i}\rangle$$

で，$a_{i1},\ a_{i2},\ \cdots\cdots,\ a_{ir_i}$ の位数が $p_i^{e_{i1}}\geqq p_i^{e_{i2}}\geqq\cdots\cdots\geqq p_i^{e_{ir_i}}$ であるとすれば，$(p_i^{e_{i1}},\ p_i^{e_{i2}},\ \cdots\cdots,\ p_i^{e_{ir_i}})$ が P_i の不変系である．

一般の有限アーベル群 G については，$G=P_1\otimes P_2\otimes\cdots\cdots\otimes P_s$ を定理10の直積分解とするとき，$P_1,\ P_2,\ \cdots\cdots,\ P_s$ の不変系をそれぞれ $(p_1^{e_1},\ p_1^{e_2},\ \cdots\cdots)$，$(p_2^{f_1},\ p_2^{f_2},\ \cdots\cdots)$，……とすれば，$G$ の不変系は
$(p_1^{e_1}p_2^{f_1}\cdots\cdots,\ p_1^{e_2}p_2^{f_2}\cdots\cdots,\ \cdots\cdots)$ である．

[定義]　不変系が $(p,\ p,\ \cdots\cdots,\ p)$ のアーベル群，つまり，

$$G=\langle a_1\rangle\otimes\langle a_2\rangle\otimes\cdots\cdots\otimes\langle a_s\rangle$$

で，各 $\langle a_i\rangle$ が位数 p の巡回群であるようなアーベル群を**基本アーベル群**という．

例題 1.　有限アーベル群 G の位数が素数 p で割り切れれば，G は位数 p の元を含む．

証明　p^α を G の位数に含まれる p の最高巾指数とし，P を G の位数が p^α の部分群とする．P はいくつかの，位数が p の巾の，巡回群の直積である．その直積因子の1つを $Q=\langle a\rangle$ とし，a の位数が p^β ならば，$a^{p^{\beta-1}}$ は位数 p の元である．

例題 2.　位数が素数 p の巾であるアーベル群が r 個の巡回群の直積であれば，$x^p=e$ をみたす元 x の個数は p^r である．

証明　$G=\langle a_1\rangle\otimes\cdots\cdots\otimes\langle a_r\rangle$ とし，a_i の位数を p^{α_i} とする．G の任意元 $x=a_1^{\lambda_1}\cdots\cdots a_r^{\lambda_r}$ $(0\leqq\lambda_i<p^{\alpha_i})$ と一意的に表される．$x^p=e\Leftrightarrow a_1^{p\lambda_1}\cdots\cdots a_r^{p\lambda_r}=e\Leftrightarrow\forall a_i^{p\lambda_i}=e\Leftrightarrow p^{\alpha_i}|p\lambda_i\Leftrightarrow\lambda_i=p^{\alpha_i-1}\mu_i$．いま $q_i=p^{\alpha_i-1}$，$b_i=a_i^{q_i}$ とおくと，$\lambda_i=q_i\mu_i$，$x=b_1^{\mu_1}\cdots\cdots b_r^{\mu_r}$ $(0\leqq\mu_i<p)$．したがって，$x^p=e\Leftrightarrow x\in\langle b_1\rangle\otimes\cdots\cdots\otimes\langle b_r\rangle$ で，このような x の個数は p^r である．

例題 3.　有限アーベル群 G は，任意の素数 p に対して $x^p=e$ となる元 x の個数が p 以下であれば，巡回群である（p. 39，例題6参照）．

証明 $|G|=p_1^{\alpha_1}\cdots\cdots p_s^{\alpha_s}$（素因数分解）とし，$P_i$ を位数 $p_i^{\alpha_i}$ の部分群とすれば，$G=P_1\otimes\cdots\cdots\otimes P_s$. いま $x^{p_i}=e$ ならば，$x\in P_i$. このような x の個数が p_i 以下であるから，P_i は巡回群である．もしも巡回群でなければ，P_i は r（$r\geqq 2$）個の巡回群の直積に分解して $x^{p_i}=e$ となる x の個数は $p_i^r>p_i$ となり矛盾を生じるからである．$(p_i, p_j)=1$，$i\neq j$，であるから，$G=P_1\otimes\cdots\cdots\otimes P_s$ は巡回群である．

例題 4． 不変系が（p, p）である基本アーベル群の自己同型群の位数を求めよ．

証明 G を不変系が（p, p）の基本アーベル群とする．G の単位元以外の p^2-1 個の元の位数は p である．G から任意の元 $a_1\neq e$ をとる．$\langle a_1\rangle$ に含まれない元 a_2 をとれば $\langle a_1\rangle\cap\langle a_2\rangle=\{e\}$ であるから，$\langle a_1\rangle\langle a_2\rangle=\langle a_1\rangle\otimes\langle a_2\rangle$ という部分群が得られる．位数を比較して，$G=\langle a_1\rangle\otimes\langle a_2\rangle$. a_1 のとり方は p^2-1 個，a_2 のとり方は p^2-p であるから，G の底のとり方は $(p^2-1)(p^2-p)$. ここで，2個の元の組でもその順序のちがうものは別の底と考えている．いま，a_1, a_2 を1つの底とし，b_1, b_2 を任意の底とすれば，対応 $a_1^{n_1}a_2^{n_2}\longmapsto b_1^{n_1}b_2^{n_2}$ は G の自己同型であり，逆に，σ を G の自己同型とするとき，$\sigma(a_i)=b_i$, $i=1, 2$, とすれば，b_1, b_2 は G の底で，$\sigma(a_1^{n_1}a_2^{n_2})=b_1^{n_1}b_2^{n_2}$ となる．したがって，G の自己同型の個数は G の底の個数 $(p^2-1)(p^2-p)$ に等しい．

注 素数 p を法とする剰余類の全体 Z_p は1つの体（付録2参照）を作っている．いま，この体を F_p で表す．上記の群 G の自己同型 σ によって $\sigma(a_1)=a_1^{i_1}a_2^{i_2}$, $\sigma(a_2)=a_1^{j_1}a_2^{j_2}$ のとき，i_1, i_2, j_1, j_2 は p を法として定まる．そこで，σ に対して，F_p の元を成分とする2行2列の行列 $\begin{pmatrix} i_1 & j_1 \\ i_2 & j_2 \end{pmatrix}$ を対応させると，この対応 φ は G の自己同型群 $A(G)$ から，F_p の元を成分とする2次の正則な，つまり行列式が0でない，行列のつくる群（F_p 上の2次の一般1次変換群）の上への同型対応になっている[1]（5-4節単純群の例参照）．

4-2-4 有限アーベル群の指標[2]

有限アーベル群 G から，0と異なる複素数のつくる乗法群 C^* への準同型を G の**指標**という．とくに G のすべての元に1を対応させる指標を**単位**

1）付録7参照．
2）付録6参照．

指標という．指標 χ, χ' の積を，

$$(\chi\chi')(a) = \chi(a)\chi'(a), \qquad a \in G,$$

で定義する．$\chi\chi'$ はまた指標である．

実際，$a, b \in G$ ならば，

$$\begin{aligned}(\chi\chi')(ab) &= \chi(ab)\chi'(ab) = \chi(a)\chi(b)\chi'(a)\chi'(b) \\ &= \chi(a)\chi'(a)\chi(b)\chi'(b) \\ &= (\chi\chi')(a)\cdot(\chi\chi')(b)\end{aligned}$$

この乗法に関して，結合法則，交換法則は成り立ち，単位指標は単位元で，指標 χ の逆元は $\chi^{-1} : a \longmapsto \chi(a)^{-1}$ であるから，指標の全体は１つのアーベル群をつくる．これを G の**指標群** $X(G)$ とよぶ．

有限アーベル群 G を巡回群の直積に分解して，

$$G = \langle a_1 \rangle \otimes \langle a_2 \rangle \otimes \cdots\cdots \otimes \langle a_r \rangle$$

とし，a_i の位数を n_i とする．χ を G の指標とすれば，G の任意の元 $a = a_1^{x_1}a_2^{x_2}\cdots\cdots a_r^{x_r}$ に対して $\chi(a) = \chi(a_1)^{x_1}\cdots\cdots\chi(a_r)^{x_r}$ であるから，χ は $a_1, a_2, \cdots\cdots, a_r$ に対する値によって定まる．また $\chi(a_i)^{n_i} = \chi(a_i^{n_i}) = \chi(e) = 1$ であるから，$\chi(a_i)$ は１の n_i 乗根である．逆に，１の n_i 乗根を ζ_i とし，$G \ni a = a_1^{x_1}\cdots\cdots a_r^{x_r}$ に $\zeta_1^{x_1}\cdots\cdots\zeta_r^{x_r}$ を対応させる写像は G の指標 χ を与え，$\chi(a_i) = \zeta_i$ となる．したがって，G は $n_1 n_2 \cdots\cdots n_r = |G|$ 個の指標をもつ．いま，ρ_i を１の原始 n_i 乗根とし，$\chi_i(a_i) = \rho_i$, $\chi_i(a_j) = 1$, $j \neq i$ とすれば，χ_i は G の指標であり，任意の指標 χ に対して $\chi(a_i) = \rho_i^{x_i}$ であれば，$\chi = \chi_1^{x_1}\chi_2^{x_2}\cdots\cdots\chi_r^{x_r}$ と唯一通りに表せる．ゆえに，指標群は $X(G) = \langle\chi_1\rangle\otimes\langle\chi_2\rangle\otimes\cdots\cdots\otimes\langle\chi_r\rangle$ と直積分解され，各 χ_i の位数は n_i である．

[定理 11]　有限アーベル群 G について $X(G) \cong G$.

[証明]　G の元 $a = a_1^{x_1}a_2^{x_2}\cdots\cdots a_r^{x_r}$ に指標 $\chi = \chi_1^{x_1}\chi_2^{x_2}\cdots\cdots\chi_r^{x_r}$ を対応させれば，G から $X(G)$ への同型を得る．

いま，a を G の元とするとき，

$$\hat{a} : \chi \longmapsto \chi(a), \qquad \chi \in X(G)$$

は $X(G)$ の指標である．実際，$\chi, \chi' \in X(G)$ のとき，

$$\hat{a}(\chi\chi') = (\chi\chi')(a) = \chi(a)\chi'(a) = (\hat{a}(\chi))(\hat{a}(\chi'))$$

$X(X(G))$ を $X^2(G)$ で表せば，定理 11 から $X^2(G) \cong X(G) \cong G$ であるが，実際対応 $a \longmapsto \hat{a}$ は G から $X^2(G)$ への同型である．まず，$\widehat{ab}(\chi) = \chi(ab) = \chi(a)\chi(b) = (\hat{a}(\chi))(\hat{b}(\chi))$ であるから $\widehat{ab} = \hat{a}\hat{b}$ で，この対応は準同型である．また，$a = a_1^{x_1} \cdots\cdots a_r^{x_r} \neq e$ ならば，ある $a_i^{x_i} \neq e$ で，このとき $\chi_i(a) = \rho_i^{x_i} \neq 1$ であるから，$\hat{a}(\chi_i) \neq 1$ で，$\hat{a}$ は$X(G)$ の単位指標ではない．したがって，$a \longmapsto \hat{a}$ の核は単位元だけからなり，この対応は G から $X^2(G)$ への同型である．G と $X(G)$, $X(G)$ と $X^2(G)$ は位数が等しいから，対応 $a \longmapsto \hat{a}$ は G から $X^2(G)$ の上への同型である．いま a と $\hat{a}$ を同一視すれば，$X^2(G) = G$ となる．これは，G が指標群 $X(G)$ の指標群とみなせることを示している．この事実を，G と $X(G)$ は**双対的**であるという．

例題 1. a, b を有限アーベル群 G の相異なる元とすれば，$\chi(a) \neq \chi(b)$ であるような G の指標が存在する．

証明 $c = ab^{-1}$ とし，$H = \langle c \rangle$ とおく．G の指標 χ が $\chi(a) = \chi(b)$ をみたせば $\chi(c) = 1$ であるから，$g \in G$, $h \in H$ のとき，$\chi(gh) = \chi(g)$．そこで χ は G/H の指標 $\bar{\chi}$ を引き起こす: $\bar{\chi}(gH) = \chi(g)$．$\chi_1(c) = \chi_2(c)$ で $\chi_1 \neq \chi_2$ ならば $\bar{\chi}_1 \neq \bar{\chi}_2$ である．逆に $\bar{\chi}$ を G/H の指標とするとき，G の元 g に対して $\chi(g) = \bar{\chi}(gH)$ とおくと，χ は G の指標であって，$\chi(h) = 1 \ \ \forall h \in H$ であり，この χ は G/H の指標 $\bar{\chi}$ を引き起こす．G/H の指標は $|G:H|$ 個あるから，$\chi(c) = 1$ となる χ は $|G:H|$ 個ある．G の指標は $|G|$ 個あり，$H \neq \{e\}$ ゆえ，$|G:H| < |G|$ であるから，$\chi(c) \neq 1$ となる χ は存在する．このとき $\chi(a) \neq \chi(b)$ である．

注 この例題は，例題のすぐ前に述べたように，$a = a_1^{x_1} \cdots\cdots a_r^{x_r} \neq e$ ならば，ある $a_i^{x_i} \neq e$ で，このとき $\chi_i(a) = \rho_i^{x_i} \neq 1$ となることからもみちびかれる．

［定理 12］ 有限アーベル群 G の指標について，つぎの関係が成り立つ．

χ が単位指標であれば，$\sum_a \chi(a) = |G|$，a は G 全体を 1 わたり動く

χ が単位指標でなければ，$\sum_a \chi(a) = 0$，a は G 全体を 1 わたり動く

a が単位元ならば，$\sum_\chi \chi(a) = |G|$，χ は G の指標すべてを 1 わた

a が単位元でなければ，　$\sum_{\chi}\chi(a)=0$，χ は G の指標すべてを1わたり動く

［証明］　χ が単位指標なら，$\chi(a)=1$ より $\sum_{a}\chi(a)=|G|$．χ が単位指標でなければ $\chi(b)\neq 1$ となる元 b が存在する．

$$\sum_{a}\chi(a)=\sum_{a}\chi(ab)=\sum_{a}\chi(a)\chi(b)$$

$$(1-\chi(b))\sum_{a}\chi(a)=0,\ \ \sum_{a}\chi(a)=0$$

$a=e$ のとき，$\chi(a)=1$ より $\sum_{\chi}\chi(a)=|G|$．$a\neq e$ のとき $\chi'(a)\neq 1$ となる χ' が存在する．

$$\sum_{\chi}\chi(a)=\sum_{\chi}\chi\chi'(a)=\sum_{\chi}\chi(a)\chi'(a)$$

$$(1-\chi'(a))\sum_{\chi}\chi(a)=0,\qquad \sum_{\chi}\chi(a)=0$$

4-3　可　解　群

有限生成アーベル群はいくつかの巡回部分群の直積に分解された．1つの群 G がいくつかの正規部分群の直積に分解されるときは，G の構造を調べることは，部分群の構造を調べることに帰着される．部分群によって群の構造を明らかにするのにもう1つの方法がある．それは G から始まって単位群 $\{e\}$ に終るある性質をもつ部分群の列

$$G=G_0\supset G_1\supset G_2\cdots\cdots\supset G_r=\{e\}$$

を用いる方法である．以下，$G_{i-1}\triangleright G_i$ で，G_{i-1}/G_i がアーベル群であるような部分群列をもつ群について考えてみよう．

いま，N は群 G の正規部分群とし，G/N がアーベル群とする．aN, bN を G/N の任意の元とすれば，$aNbN=bNaN$ であるから，$abN=baN$，$ab(ba)^{-1}=aba^{-1}b^{-1}\in N$ となり，N は G の任意の元 a,b に対し，$aba^{-1}b^{-1}$ という形の元をすべて含まなければならない．いま，$aba^{-1}b^{-1}$ を a, b の**交換子**といって，$[a, b]$ で表す．すべての交換子から生成された群を G の**交換子群**といって，$D(G)$ で表すことにすれば，つぎの定理が得られる．

[定理 13] Nを群 G の部分群とする. Nが G の正規部分群で, G/N がアーベル群であるための必要十分条件は N が G の交換子群 $D(G)$ を含むことである. とくに, G の交換子群 $D(G)$ は正規部分群である.

[証明] 必要なことは上に述べた. 十分であることをいう. $G>N$ で, $N\supset D(G)$ とする. Nの任意の元 x に対して $axa^{-1}=axa^{-1}x^{-1}x\in D(G)x\subset N$ であるから, $N \lhd G$. また $ba=abb^{-1}a^{-1}ba=ab[b^{-1}, a^{-1}]$, $baN=abN$, $bNaN=aNbN$ となり, G/N はアーベル群である. $c[a, b]c^{-1}=[cac^{-1}, cbc^{-1}]$ であるから, $D(G)\lhd G$.

問 1. (1) $[a, b]=e \Leftrightarrow ab=ba$

(2) $[b, a]=[a, b]^{-1}$

(3) $c[a, b]c^{-1}=[cac^{-1}, cbc^{-1}]$

問 2. H, K が群 G の正規部分群で, G/H, G/K がアーベル群ならば, $G/(H\cap K)$ もアーベル群である.

例題 1. 対称群 $\mathfrak{S}_n$ の交換子群は交代群 $\mathfrak{A}_n$ に一致する.

証明 $\mathfrak{S}_n/\mathfrak{A}_n$ は位数2であるから巡回群で, $D(\mathfrak{S}_n)\subset\mathfrak{A}_n$. 一方, $\mathfrak{A}_n$ は, 長さ3の巡回置換 $(\alpha\ \beta\ \gamma)$ で生成され (p. 28, 例題4), $(\alpha\ \beta\ \gamma)=(\alpha\ \beta)(\alpha\ \gamma)(\alpha\ \beta)^{-1}(\alpha\ \gamma)^{-1}$ であるから, $\mathfrak{A}_n\subset D(\mathfrak{S}_n)$. したがって, $\mathfrak{A}_n=D(\mathfrak{S}_n)$.

さて, 群 G の部分群の列

$$(G) \qquad G=G_0\supset G_1\supset G_2\cdots\cdots\supset G_r=\{e\}$$

において各 G_i は G_{i-1} の正規部分群のとき, この列を G の**正規鎖**[1]といい, 正規鎖から得られる剰余群の列

$$G_0/G_1,\ G_1/G_2,\ \cdots\cdots,\ G_{r-1}/G_r(=G_{r-1})$$

をその**剰余群列**という.

[定義] 群 G の正規鎖 (G) において, G_{i-1}/G_i がすべてアーベル群のとき, (G) を**可換正規鎖**という. 群 G が少なくとも1つ可換正規鎖をもつとき G を**可解群**という.

アーベル群は可換正規鎖 $G\supset\{e\}$ をもつから, 可解群である.

例題 2. 可解な単純群は位数が素数の巡回群である.

1) 付録3参照.

証明　$G \neq \{e\}$ が可解群ならば，可換正規鎖 $G=G_0=G_1=\cdots\cdots=G_{i-1}\supset G_i\cdots\cdots\supset\{e\}$ をもつから，交換子群 $D(G)\subset G_i$ で，$D(G)$ は G と異なる正規部分群である．G が単純群ならば，$D(G)=\{e\}$．したがって，G はアーベル群である．アーベル群の部分群はすべて正規部分群であるから，G は真の部分群を含まない．したがって，$G\ni a\neq e$ とすれば，$G=\langle a\rangle$．G が無限巡回群ならば，$\langle a^2\rangle$ は G の真の部分群となるから，G は位数が有限 n の巡回群である．n が素数でなければ，その素因子の 1 つを p とすれば，$\langle a^p\rangle$ は位数が n/p の真の部分群になるから，n は素数でなければならない．

例題 3.　4 次以下の対称群はすべて可解群である．

証明　$\mathfrak{S}_2$ は位数 2 の巡回群であるから可解群である．$\mathfrak{S}_3$ については，$\mathfrak{S}_3\supset\mathfrak{A}_3\supset\{e\}$ は可換正規鎖であるから，$\mathfrak{S}_3$ は可解群である．$\mathfrak{S}_4$ については，$V=\{e,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$ は位数 4 のアーベル群であり，$\mathfrak{A}_4$ の（実は $\mathfrak{S}_4$ の）正規部分群である（p. 69，例題 1）．部分群列 $\mathfrak{S}_4\supset\mathfrak{A}_4\supset V\supset\{e\}$ において，$\mathfrak{S}_4/\mathfrak{A}_4$ は位数 2 の，$\mathfrak{A}_4/V$ は位数 3 の巡回群，V はアーベル群であるから，この部分群列は可換正規鎖である．したがって $\mathfrak{S}_4$ は可解群である．

問 3.　4 次交代群 $\mathfrak{A}_4$ の交換子群 $D(\mathfrak{A}_4)=V$.

[定理 14]　H を群 G の部分群とする．

(G)　$G=G_0\supset G_1\supset G_2\cdots\cdots\supset G_r=\{e\}$

が G の正規鎖であれば，

(H)　$H=H\cap G_0\supset H\cap G_1\supset\cdots\cdots\supset H\cap G_r=\{e\}$

は H の正規鎖である．また (G) が可換正規鎖ならば，(H) も可換正規鎖である．したがって，可解群の部分群は可解群である．

[**証明**]　$H\cap G_{i-1}$ の任意元 x と $H\cap G_i$ の任意元 y について，$x\in G_{i-1}$, $y\in G_i\lhd G_{i-1}$ であるから，$xyx^{-1}\in G_i$．$x, y\in H$ であるから，$xyx^{-1}\in H$．したがって，$xyx^{-1}\in H\cap G_i$, $H\cap G_i\lhd H\cap G_{i-1}$．$H\cap G_{i-1}=H_{i-1}$, $H\cap G_i=H_i$ とおくと，$G_{i-1}\rhd G_i$, $G_{i-1}>H_{i-1}$, $H_{i-1}\cap G_i=H\cap G_{i-1}\cap G_i=H\cap G_i=H_i$ で，第 2 同型定理によって，G_{i-1}/G_i の部分群 $H_{i-1}G_i/G_i$ は $H_{i-1}/H_{i-1}\cap G_i=H_{i-1}/H_i$ に同型である．したがって，もしも G_{i-1}/G_i がアーベル群ならば H_{i-1}/H_i もアーベル群で，(G) が可換正規鎖ならば，(H) も可換正規鎖である．

[定理 15]　N は群 G の正規部分群で，N と G/N が可解群であれば，G 自身可解群である．

問 4. 上の定理を証明せよ.

例題 4. 交代群 $\mathfrak{A}_n(n\geqq 5)$ は非可解な単純群である. したがって, 対称群 $\mathfrak{S}_n(n\geqq 5)$ は可解群でない.

証明 まず, はじめに, $n\geqq 5$ のとき, $\mathfrak{S}_n>H, N, H\triangleright N$ で, H がすべての 3 項巡回置換を含み, H/N がアーベル群ならば, N はすべての 3 項巡回置換を含むことを示す. H/N がアーベル群であるから, N は H の交換子群 $D(H)$ を含む. 文字の個数 $n\geqq 5$ であるから, i, j, k, r, s を異なる文字とし, $\sigma=(i\ j\ k)$, $\tau=(k\ r\ s)$ とすれば, $[\sigma, \tau]=(i\ r\ k)\in N$. i, r, k をあらかじめとったとき, j, s を補助にとれるわけだから, 任意の 3 項巡回置換は N に入る.

さて, いまかりに $\mathfrak{A}_n=H_0\supset H_1\supset\cdots\cdots\supset H_r=\{e\}$ を可換正規鎖とすれば, $\mathfrak{A}_n$ はすべての 3 項巡回置換 $(\alpha\ \beta\ \gamma)=(\alpha\ \gamma)(\alpha\ \beta)$ を含み, H_0/H_1 がアーベル群であるから, H_1 はすべての 3 項巡回置換を含む. 以下同様にして, 最後に $H_\nu=\{e\}$ がすべての 3 項巡回置換を含むことになって, 矛盾を生じる. したがって, $\mathfrak{A}_n$ は可換正規鎖をもたず, $\mathfrak{A}_n$ は非可解である. $\mathfrak{S}_n$ の非可解性も同様にして示される.

しかし, $\mathfrak{A}_n$ の単純性がわかれば, $\mathfrak{A}_n$ は非可換であるから, $\mathfrak{A}_n$ は非可解であり, $\mathfrak{S}_n$ も, 定理 14 から, 非可解となる.

つぎに, $\mathfrak{A}_n$ の単純性を示す. $N\neq\{e\}$ を $\mathfrak{A}_n$ の正規部分群として $N=\mathfrak{A}_n$ を示せばよい. そのために, N の e 以外の元で, それが動かす文字が最も少ないものを σ とすれば, σ は 3 項巡回置換であることを示す. かりに σ は 3 項巡回置換でなく, 少なくとも 4 個の文字を動かすとする. σ を共通の文字を含まない巡回置換の積に分解すれば,

(1) $\sigma=(1\ 2)(3\ 4)\cdots\cdots$か, 長さが少なくとも 3 の巡回置換を含む

(2) $\sigma=(1\ 2\ 3\cdots\cdots)\cdots\cdots$(文字の書き変えだから, このようにしてよい).

(2) の場合 4 文字しか動かさないとすると, $\sigma=(1\ 2\ 3\ 4)=(1\ 4)(1\ 3)(1\ 2)$ は奇置換であるから矛盾であるので, この場合は, 1, 2, 3, 4, 5 は動くとしてよい. さて, $\tau=(3\ 4\ 5)\in\mathfrak{A}_n$ とすると, 各場合について

(1) $\sigma_1=\tau\sigma\tau^{-1}=(1\ 2)(4\ 5)\cdots\cdots$

(2) $\sigma_1=\tau\sigma\tau^{-1}=(1\ 2\ 4\cdots\cdots)\cdots\cdots$

となって, $\sigma_1^{-1}\sigma\neq e$. $k>5$ が σ で不変であれば, $\tau(k)=k$ であるから, $\sigma_1^{-1}\sigma(k)=k$ であり, (1), (2) のいずれの場合も $\sigma_1^{-1}\sigma(1)=1$. さらに (1) の場合には $\sigma_1^{-1}\sigma(2)=2$ で

あるから，$\sigma_1^{-1}\sigma$ の動かす文字は σ の動かす文字より少なくなって，σ のとり方に反する．したがって，σ は3項巡回置換で，$\sigma=(1\ 2\ 3)$ としてよい．

i, j, k を任意の異なる3文字とするとき，$\rho: 1\longmapsto i, 2\longmapsto j, 3\longmapsto k$ となる元 $\rho\in\mathfrak{S}_n$ をとる．ρ が奇置換なら，$(n-1, n)\rho$ を改めて ρ とすれば，$\rho\in\mathfrak{A}_n$ としてよい．このとき，$\rho\sigma\rho^{-1}=(i\ j\ k)\in N$ であって，N は任意の3項巡回置換を含むから，p. 28 例題4により $N=\mathfrak{A}_n$ となる．

問 5.　$\mathfrak{S}_n (n\geqq 5)$ の正規部分群は $\mathfrak{A}_n$ 以外にない．

問 6.　5次対称群 $\mathfrak{S}_5$ は非可解群である．また，このことから，$\mathfrak{S}_n$, $n\geqq 5$ は非可解群であることをみちびけ．

注　例題4はガロアによって証明された．5次以上の一般代数方程式は有理演算と巾根演算を有限回使っては，つまり代数的には解けないという方程式論の基本定理で重要な役割を演じている．可解群という名もそれに由来している．

[定理 16]　可解群の準同型像は可解群である．とくに，可解群の剰余群は可解群である．

[証明]　G を可解群とし，$\varphi(G)=G'$ を準同型像とする．G の可換正規鎖を $G=G_0\supset G_1\supset\cdots\cdots\supset G_r=\{e\}$ とする．$\varphi(G_i)=G_i'$ とすれば，(G')　$G'=G_0'\supset G_1'\supset\cdots\cdots\supset G_r'=\{e'\}$ は G' の正規鎖である．G'_{i-1}/G_i' の任意の元 $x'G_i'$, $y'G_i'$ をとると，$x'=\varphi(x)$, $y'=\varphi(y)$, $x, y\in G_{i-1}$ で，$xyx^{-1}y^{-1}\in G_i$ であるから，$x'y'x'^{-1}y'^{-1}=\varphi(xyx^{-1}y^{-1})\in\varphi(G_i)=G_i'$ となって，G'_{i-1}/G_i' はアーベル群である．したがって，(G') は G' の可換正規鎖であり，G' は可解群である．

[定理 17]　可解群 G_1, G_2 の直積 $G_1\otimes G_2$ は可解群である．

問 7.　上の定理を証明せよ．

問　題　4

1. H, K は群 G の部分群で $HK=H\otimes K$ ならば，$H\otimes K/K\cong H$ である．
2. $G=H\otimes K$ ならば，G の中心 $Z(G)=Z(H)\otimes Z(K)$.
3. $G=H\otimes K$ ならば，G の交換子群 $D(G)=D(H)\otimes D(K)$.
4. $N_1, N_2, \cdots\cdots, N_r$ は群 G の正規部分群で，$N_1\cap N_2\cap\cdots\cdots\cap N_r=\{e\}$ ならば，G は $G_1/N_1\otimes G_2/N_2\otimes\cdots\cdots\otimes G_r/N_r$ の部分群に同型である．

5. H, K が群 G の正規部分群で，$H \cap K = \{e\}$ とする．G/H, G/K が可解群であれば，G は可解群である．

6. M, N は群 G の正規部分群で，$G=MN$ であれば $G/(M \cap N)$ は $G/M \otimes G/N$ に同型である．

7. H は $G=G_1 \otimes G_2$ の部分群とする．H の元 $b=a_1a_2$ $(a_1 \in G_1,\ a_2 \in G_2)$ の G_1 成分 a_1 の全体を $\overline{H}_1$, G_2 成分 a_2 の全体を $\overline{H}_2$ とする．また，$H_1=H \cap G_1$, $H_2=H \cap G_2$ とおく．各 $\overline{H}_i$ は G_i の部分群であり，$H_i \lhd \overline{H}_i$ である．また，$\overline{H}_1/H_1 \cong \overline{H}_2/H_2$.

8. $G=G_1 \otimes G_2$ において，$|G_1|$ と $|G_2|$ が互いに素であれば，G の任意の部分群 H に対して $H=H_1 \otimes H_2$．ここで，$H_i=H \cap G_i$, $i=1, 2$.

9. 群 G_1 の位数と群 G_2 の位数が互いに素であれば

$$\text{自己同型群 } A(G_1 \otimes G_2) \cong A(G_1) \otimes A(G_2)$$

注　クラインの四元群 $V=\langle a\rangle \otimes \langle b\rangle$, $a^2=b^2=e$ については $A(V) \cong \mathfrak{S}_3$ となる（問題3の8）から，$|G_1|$ と $|G_2|$ が互いに素でないときは，この9番にいう同型は必ずしも成り立たない．

10. 有限アーベル群 G の不変系が (p^5, p^3, p^2, p, p) であれば $G^{(p)}=\{a^p, a \in G\}$ の不変系は (p^4, p^2, p) である．

11. 有限アーベル群 G の不変系を $(q_1, q_2, \cdots\cdots, q_s)$ とする．いま，$q_1', q_2', \cdots\cdots, q_t'$，$(t \leqq s)$，は $q'_k | q'_{k-1}$, $1 \leqq k \leqq t$，で $q_i' | q_i$ という正整数の列とすれば，$(q_1', q_2', \cdots\cdots, q_t')$ を不変系にもつ G の部分群と，G に準同型な群が存在する．

12. p を素数とする．有限アーベル群 G において $x^p=e \quad \forall x \in G$ であれば，G は基本アーベル群である．

13. 不変系が (p, p, p, p) の基本アーベル群 G の位数が p^2 の部分群の個数と，位数が p^3 の部分群の個数を求めよ．

14. G は有限アーベル群で，G の元の位数の最大値を m とすれば，

$$x^m = e \quad \forall x \in G$$

15. G は位数 n の有限アーベル群とする．G は，n の任意の約数 m に対して，位数 m の部分群をもつ．

16. G は有限アーベル群，G^* は G の指標群とする．

(1) H を G の部分群とすると，

$$G_H{}^* = \{\chi | \chi \in G^*,\ \chi(h) = 1,\ \forall h \in H\}$$

は G^* の部分群であり，$G_H{}^* \cong G/H$

(2) H^* を G^* の部分群とすると，

$$G_{H^*} = \{a | a \in G,\ \chi(a) = 1,\ \forall\chi \in H^*\}$$

は G の部分群であり，$G_{H^*} \cong G^*/H^*$

17. H は群 G の部分群，N は G の正規部分群で，$G=HN$ とする．H, N がともに可解群であれば，G は可解群である．

18. $n \geqq 5$ のとき n 次交代群 $\mathfrak{A}_n$ の交換子群 $D(\mathfrak{A}_n)=\mathfrak{A}_n$ である．これより，$\mathfrak{S}_n$ $(n \geqq 5)$ が非可解群であることをみちびけ．

5

有　限　群

5-1　シローの定理

この章ではとくに断らないかぎり群といえば有限群のこととし，有限群に固有な性質について述べる．群 G の部分群の位数は G の位数の約数であるが，G の位数 g の任意の約数を位数とする部分群は必ずしも存在しない(p. 61)．しかし，h が g を割る素数の巾のときは，位数 h の部分群が少なくとも1つ存在する．とくに，h が g を割る素数の最高巾 p^r のとき，位数 p^r の部分群を G の **p-シロー群**という．p-シロー群の性質は有限群の構造を調べる上で最も基本的である．

以下，p は素数を表すとして，位数が p の巾である群を **p-群**という．群 G の部分群が p-群のとき，これを G の **p-部分群**という．G の p-シロー群は，指数が p と素な p-部分群である．p-部分群（p-シロー群）に共役な部分群は p-部分群（p-シロー群）である．

［定理 1］　有限群 G の G と異なるすべての部分群の指数が素数 p で割り切れれば，G の中心 Z の位数は p で割り切れる．とくに $Z \neq \{e\}$．

［証明］　$|G|=g$ として，その類公式を，

$$g = z + h_{z+1} + \cdots\cdots + h_k \quad (z = |Z|,\ h_i > 1)$$

とすると，h_i はある元 a_i に共役な元の個数で，a_i の正規化群を $N(a_i)$ とするとき，$h_i = |G : N(a_i)|$ である．g, 各 h_i は p で割り切れるから，z も p で割り切れる．

［定理 2］　（シローの定理 I）

群 G の位数が素数巾 p^s で割り切れれば，G は位数 p^s の部分群を含む．

［証明］　G の位数が p のときは明らかである．G の位数に関する帰納法で証明

する.

(i)　$|G:H|$ が p で割れないような真の部分群 H が存在するときは, H の位数は p^s で割れるから, 帰納法の仮定により, H は位数 p^s の部分群をもつ. これは G の部分群であるから, 定理は成り立つ.

(ii)　G と異なるすべての部分群の指数が p で割り切れるなら, G の中心 Z の位数は p で割れる. Z はアーベル群であるから, Z は位数 p の部分群 P を含む. $P \lhd G$ で, G/P の位数は $|G|$ より小さく, また p^{s-1} で割れるから, 帰納法の仮定により, G/P は位数が p^{s-1} の部分群 $\bar{U}=U/P$ を含む. このとき U は位数 p^s の G の部分群である.

[系]　(コーシー)

群 G の位数が素数 p で割れれば, G は位数 p の元を含む.

定理2から, G の位数を割る p の最高巾を p^r とすれば, G は位数 p^r の部分群を含む. 以下, G の p-シロー群を $S(p)$, S_p または P などで表す.

[定理 3]　(シローの定理II)

U を群 G の p-部分群とすれば, U を含む G の p-シロー群が存在する.

[定理 4]　(シローの定理III)

群 G の p-シロー群はすべて互いに共役である.

[証明]　2つの定理を同時に証明する. S_p を1つの p-シロー群とし, S_p と U による両側分解を $G=S_px_1U+\cdots\cdots+S_px_rU$ とすると, S_px_iU に含まれる S_p の左剰余類の個数は,

$$p^{e_i}=|U:U\cap x_i^{-1}S_px_i|$$

であるから, $|G:S_p|=p^{e_1}+\cdots\cdots+p^{e_r}$. 左辺は p と素であるから, ある i に対して $p^{e_i}=1$. このとき $U=U\cap x_i^{-1}S_px_i$, すなわち, $U\subset x_i^{-1}S_px_i$ で, $x_i^{-1}S_px_i$ は U を含む G の p-シロー群である. とくに, U が p-シロー群ならば, 位数を比較して $U=x_i^{-1}S_px_i$ すなわち, U と S_p は共役である.

[系]　群 G の p-シロー群 S_p が正規部分群ならば, S_p は G の唯一つの p-シロー群である.

問 1.　N が群 G の正規 p-部分群ならば, N は G の任意の p-シロー群に含まれる.

［定理 5］ （シローの定理Ⅳ）

群 G の異なる p-シロー群の個数 n_p は p を法として1と合同である．すなわち $n_p=1+kp$ となる．

［証明］ P を G の1つの p-シロー群とすると，G の任意の p-シロー群は P に共役ゆえ，異なる p-シロー群の個数 n_p は P に共役な部分群の個数 $|G:N(P)|$ に等しい．G の $N(P)$ と P による両側分解を $G=N(P)x_1P+\cdots\cdots+N(P)x_tP$, $x_1=e$ とし，$p^{e_i}=|P:P\cap x_i^{-1}N(P)x_i|$ とすれば，p^{e_i} は $N(P)x_iP$ に含まれる $N(P)$ の左剰余類の個数に等しい．$p^{e_1}=1$ であるから，$|G:N(P)|=1+p^{e_2}+\cdots\cdots+p^{e_t}$. したがって，$e_i>0$, $i=2, \cdots\cdots, t$ がいえればよい．いま，ある $i\geqq 2$ に対して $p^{e_i}=1$ とすれば，$P\subset x_i^{-1}N(P)x_i$, $x_iPx_i^{-1}\subset N(P)$ となり，P も $x_iPx_i^{-1}$ も $N(P)$ の p-シロー群である．$P\lhd N(P)$ であるから，上の系によって，$P=x_iPx_i^{-1}$, したがって $x_i\in N(P)$. このとき，$N(P)x_i\,P=N(P)x_1P$ となって，$i\geqq 2$ という仮定に反する．したがって，$e_i>0$, $\forall i\geqq 2$ である．

［定理 6］ S_p を群 G のp-シロー群，N を G の正規部分群とすると，

(1) $S_p\cap N$ は N の p-シロー群である．

(2) S_pN/N は G/N の p-シロー群である．

［証明］ $S_pN/N\cong S_p/S_p\cap N$ より，S_pN/N は p-群である．$|G/N:S_pN/N|=|G:S_pN|$ は p と素であるから，S_pN/N は G/N の p-シロー群である．

つぎに，$S_p\cap N$ は N の p-部分群である．S_pN は G の部分群であるから，p. 46, 定理9, 系1より，$S_p\cap N$ の指数 $|N:S_p\cap N|=|S_pN:S_p|$ で，これは p と素であるから，$S_p\cap N$ は N の p-シロー群である．

問 2. 群 G の正規部分群 N の指数が，G の位数の1つの素因子 p と素であれば，G の任意の p-シロー群は N に含まれる．

例題 1. 群 G の p-シロー群 P の各元と交換可能な2つの元 a, b が G で共役であれば，a, b は $N(P)$ で共役である．

証明 仮定により，$P\subset N(a)$, $P\subset N(b)$. いま，$b=xax^{-1}$, $x\in G$ より，$xPx^{-1}\subset xN(a)x^{-1}=N(b)$, P も xPx^{-1} も $N(b)$ のp-シロー群．したがって，$P=uxPx^{-1}u^{-1}$, $u\in N(b)$, $ux\in N(P)$ である．そこで，$(ux)a(ux)^{-1}=ubu^{-1}=b$.

以下，シローの定理を応用したいくつかの例題をあげる．はじめに，つぎの補助定理（p. 49，定理 11）を注意しておく．

[補助定理]　有限群 G の部分群 H の共役群の個数は $|G:N(H)|$ に等しい．したがって，共役群の個数は，$|G:H|$ の約数である．

例 1.　位数 33 の群の 3-シロー群，11-シロー群は正規部分群である．

証明　3-シロー群 S_3 の共役の個数は $1+3k$ と表され，$33/3=11$ の約数であるから，1．したがって，S_3 は正規部分群．11-シロー群 S_{11} の共役の個数は $1+11k$ と表され，$33/11=3$ の約数であるから，1．したがって S_{11} は正規部分群．

問 3.　つぎの各場合，群 G のシロー群はいくつあるか．

(1)　$|G|=91$　　(2)　$|G|=323$

問 4.　位数が pq（p, q は素数で，$q<p$）の群 G の p-シロー群は正規部分群である．

例題 2.　位数が 56 の群は単純群でない．

証明　位数 56 の群を G とし，G が単純群とする．G の 7-シロー群 Q の共役の個数 $n_7=1+7k>1$ で，$56/7=8$ の約数であるから，$n_7=8$．Q とその共役は単位元 e だけを共有するから，8 個の 7-シロー群の和集合は $(7-1)\times8+1=49$ 個の元を含む．8 個の 7-シロー群と 8 個の元からなる 2-シロー群 1 つとで G 全体になるから，2-シロー群は唯一つしか存在せず，2-シロー群は正規部分群であり，G が単純群であることに矛盾する．

例 2.　位数が 20 の群は可解群である．

証明　位数 20 の群を G とする．5-シロー群の共役の個数は 1 であるから，$S_5\lhd G$．S_5, G/S_5 ともにアーベル群であるから，$G\rhd S_5\rhd\{e\}$ は可換正規鎖で，G は可解群である．

問 5.　つぎの各場合，群 G は可解群である．$n=|G|$ とする．

(1)　$n=2^2\cdot7$　　(2)　$n=2\cdot3^2$　　(3)　$n=3^2\cdot5$

(4)　$n=2^3\cdot11$　　(5)　$n=80$　　(6)　$n=459$

(7)　$n=992$（p-群は可解群であることを使え．このことは，あとで，p. 111，定理 12 で示す）

例題 3.　位数 6 の群は巡回群であるか，3 次対称群 $\mathfrak{S}_3$ に同型である．

証明　G の 2-シロー群を S_2, 3-シロー群を S_3 とする．$|G:S_3|=2$ より $S_3\lhd G$．したがって，S_3S_2 は G の部分群であり，$S_3\cap S_2=\{e\}$ であるから，S_3S_2 の元は uv,

$u\in S_3$, $v\in S_2$, と1通りに表せ，$S_3S_2=G$. S_3, S_2 はともに巡回群で，その生成元をそれぞれ a, b とすれば，G の元は a^mb^n, $m=0, 1, 2$, $n=0, 1$ と1通りに表せる．$bab^{-1}\in S_3$ である．

(i) $bab^{-1}=a$, つまり $ba=ab$ ならば，$G=S_3\otimes S_2$ で, G は位数6の巡回群である．

(ii) $bab^{-1}=a^2$, つまり $a^2b=ba$ ならば, G は3次対称群と同型である．(それには位数3の元 a には位数3の $\sigma=(1\ 2\ 3)$ を，位数2の元 b には位数2の $\tau=(1\ 2)$ を対応させればよい．)

例題 4. 位数45の群 G はアーベル群である．

証明 G の3-シロー群を S_3, 5-シロー群を S_5 とする．S_3 の共役群の個数 n_3 は $1+3k$ で，$45/3^2=5$ の約数であるから，1に等しく，したがって $S_3\lhd G$. 同様にして $S_5\lhd G$ がわかる．S_3S_5 は G の部分群で，$S_3\cap S_5=\{e\}$ であるから，$S_3S_5=G$. S_3, S_5 ともに G の正規部分群であるから $G=S_3\otimes S_5$. S_3 は位数 3^2 の群であるからアーベル群，S_5 は巡回群．ゆえに G はアーベル群．

問 6. つぎの各場合，群 G は巡回群である．

(1) $|G|=33$　(2) $|G|=91$　(3) $|G|=119$

例題 5. 位数が pq (p, q はともに素数で $p>q$) の群 G を決定せよ．

解 G の p-シロー群を P とすると，P の共役群の個数 n_p は $1+kp$ で，$n_p|q$ であるが，$q<p$ であるから，$n_p=1$. したがって $P\lhd G$. q-シロー群を Q とすれば $PQ<G$. $P\cap Q=\{e\}$ であるから $PQ=G$. いま，$P=\langle a\rangle$, $Q=\langle b\rangle$ とする．$P\lhd G$ であるから，$bab^{-1}=a^\mu$ で，μ は法 p の既約剰余類を決める．$a=b^qab^{-q}=a^{\mu^q}$ であるから，$\mu^q\equiv 1 \pmod{p}$. したがって $q\nmid p-1$ のときは $\mu\equiv 1$ で，このときは $bab^{-1}=a$ となり，P の元と Q の元は可換で，$Q\lhd G$, $G=P\otimes Q$ となり，G は巡回群である．$q|p-1$ であっても $\mu\equiv 1 \pmod{p}$ ならば，G は巡回群である．$q|p-1$ で $\mu\not\equiv 1 \pmod{p}$ のときは G は非アーベル群で，Q の共役は p 個ある．このとき，$b\longmapsto\mu$ は Q から法 p の既約剰余類群 $\boldsymbol{Z}_p{}^*$ の中への同型である．さて，$a^p=b^q=e$, $bab^{-1}=a^\mu$ で定義された群と，$a'^p=b'^q=e'$, $b'a'b'^{-1}=a'^{\mu'}$ で定義された群の間には，つぎのような同型が成り立つ．$b\longmapsto\mu$, $b'\longmapsto\mu'$ により，$Q=\langle b\rangle$ も $Q'=\langle b'\rangle$ も巡回群 $\boldsymbol{Z}_p{}^*$ の唯一つの位数 q の部分群にうつるから，$\langle\mu\rangle=\langle\mu'\rangle$. したがって $\mu'\equiv\mu^k \pmod{p}$, k は q と素となる．そこで，$\varphi(a')=a$, $\varphi(b')=b^k$ とすれば，$\varphi(b'a'b'^{-1})=\varphi(a'^{\mu'})=a^{\mu'}=a^{\mu^k}=b^kab^{-k}=\varphi(b')\varphi(a')\varphi(b')^{-1}$ であって，この2つの群は同型になる．以上まとめて，位数 pq の群は $q\nmid p-1$ のとき，巡回群に限り，$q|p-1$ のときは，巡回群の他に唯一つの型の

非可換な可解群が存在する．

例題 6.　4次対称群 $\mathfrak{S}_4$ の部分群をすべて求めよ．

解　$|\mathfrak{S}_4|=24$ であるから，真の部分群の位数は 2, 3, 4, 6, 8, 12 のいずれかである．

位数 2：位数 2 の各元によって 1 つずつつくられる．(1 2) 型の元から 6 個，(1 2) (3 4) 型のものから 3 個．

位数 3：位数 3 の元は (1 2 3) 型で，全体で 8 個ある．これから $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ の型の部分群が 4 個得られる．これらは 3-シロー群で，互いに共役である．

位数 4：i)　巡回群は (1 2 3 4), (1 3 4 2), (1 4 2 3) のそれぞれが生成する 3 個．

ii)　非巡回群は，可換な位数 2 の 2 つの元で生成されるもので，正規部分群である．

$$V=\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

と $U=\{e, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}$ の型のもの 3 個．

位数 8：これは 2-シロー群であるから，互いに共役である．その個数は 1 か 3 かである．実はつぎに示すように 3 である．まず，位数 4 の V は 1 つの 2-シロー群に含まれるが，V は正規部分群であるから，すべての 2-シロー群は V を含む．いま，$(1\ 2\ 3\ 4)\notin V$, $(1\ 2\ 3\ 4)^2=(1\ 3)(2\ 4)\in V$ ゆえ，$(1\ 2\ 3\ 4)\ V\cup V$ は位数 8 の部分群 $P_2=\{V, (1\ 2\ 3\ 4), (1\ 3), (1\ 4\ 3\ 2), (2\ 4)\}$ をつくる．(1 2 3 4) の代りに (1 3 4 2), (1 4 2 3) のそれぞれを使って 2-シロー群 P_2', P_2'' が得られる．以上で 3 個．

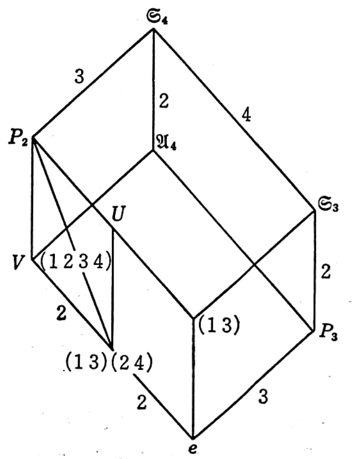


図 5-1

位数 6：位数 6 の部分群は位数 3 の部分群を含み，この位数 3 の部分群は，指数 2 であるから，正規部分群である．したがって，位数 6 の部分群は，先の位数 3 の部分群の正規化群に含まれている．一方，位数 3 の部分群の共役は 4 個であるから，この正規化群の位数は 6 である．したがって，位数 6 の部分群は多くとも 4 個である．具体的には

文字4を固定する置換全体（$\cong\mathfrak{S}_3$）．この型のものは4個ある．

位数12：交代群 $\mathfrak{A}_4$ は位数12である．この他には存在しない．もしも $H\neq\mathfrak{A}_4$ も位数12の部分群とすれば，$\mathfrak{A}_4H=\mathfrak{S}_4$ であるから，$\mathfrak{S}_4/\mathfrak{A}_4=\mathfrak{A}_4H/\mathfrak{A}_4\cong H/\mathfrak{A}_4\cap H$ であって，$\mathfrak{A}_4\cap H$ は位数が6の群であり，しかも偶置換だけからなる．一方，上に見たように位数6の部分群はすべて奇置換を含むから，これは矛盾である．

$\mathfrak{S}_4$ の部分群の包含関係は前ページの図の様になる．真の正規部分群は $\mathfrak{A}_4$ と V のみ．P_2, P_3 は2-シロー群．3-シロー群．$\mathfrak{A}_4$ と V 以外の部分群は互いに共役なもののうちの1つを代表して示してある．

5-2 可解群・巾零群

5-2-1 交換子群列・可解群[1)]

ここでは群は有限群とかぎらない．

群 G の部分群 H, K に対して，H の元 h と K の元 k の交換子 $hkh^{-1}k^{-1}=[h, k]$ の全体から生成された部分群を **H と K の交換子群**といい，記号 $[H, K]$ で表す．$[h, k]^{-1}=(hkh^{-1}k^{-1})^{-1}=khk^{-1}h^{-1}=[k, h]$ であるから，$[H, K]=[K, H]$ である．$H\lhd G$ であれば $h(kh^{-1}k^{-1})\in H$ であるから，$[H, K]\subset H$．さらに，$K\lhd G$ であれば，$[H, K]\subset H\cap K$．また $x[h, k]x^{-1}=[xhx^{-1}, xkx^{-1}]$ であるから，$H\lhd G$, $K\lhd G$ であれば，$[H, K]\lhd G$.

群 G の交換子群 $D(G)$ は $[G, G]$ のことである．先に，p. 95，定理13で述べたように，$D(G)$ は G/N がアーベル群となるような正規部分群 N のすべてに含まれている，最小のものである．

群 G の交換子群 $D(G)=D_1(G)$, $D_1(G)$ の交換子群を $D_2(G)$ とし，一般に，$D_{i+1}(G)=[D_i(G), D_i(G)]$ とすれば，G の正規部分群の列

$$G\supset D_1(G)\supset D_2(G)\supset \cdots\cdots D_i(G)\supset\cdots\cdots$$

を得る．この列を G の**交換子群列**という．ここで，各 $D_i(G)/D_{i+1}(G)$ はアーベル群である．

1) 巻末文献〔3〕,〔6〕,〔7〕,〔9〕参照.

先に 4-3 節で，群 G は可換正規鎖

$$G = G_0 \supset G_1 \cdots\cdots \supset G_r = \{e\}$$

ここで，$G_i \triangleright G_{i+1}$, G_i/G_{i+1} はアーベル群である，をもつとき，可解群と定義した．さて，つぎの定理が成り立つ．

[定理 7] 群 G が可解群であるための必要十分条件は，G の交換子群列において，ある r に対し $D_r(G) = \{e\}$ となることである．

[証明] G が可解群とすれば，可換正規鎖において，G/G_1 はアーベル群であるから $G_1 \supset D(G) = D_1(G)$．いま，$G_{i-1} \supset D_{i-1}(G)$ を仮定すれば，G_{i-1}/G_i がアーベル群であるから，$G_i \supset [G_{i-1}, G_{i-1}] \supset [D_{i-1}(G), D_{i-1}(G)] = D_i(G)$ となる．帰納法によって，一般に，$G_j \supset D_j(G)$ が証明される．とくに，$G_r = \{e\}$ であるから，$D_r(G) = \{e\}$ となる．

逆に交換子群列において，$D_r(G) = \{e\}$ であるとする．交換子群列は正規鎖であり，各 $D_i(G)/D_{i+1}(G)$ はアーベル群であるから，交換子群列は可換正規鎖である．したがって，G は可解群である．

つぎの定理はすでに 4-3 節で述べてあるが，別証明を与える．

[定理 8] 可解群 G の部分群，剰余群はそれぞれ可解群である．

[証明] H を G の部分群とする．$D_1(G) = [G, G] \supset [H, H] = D_1(H)$．つぎに，$D_2(G) = [D_1(G), D_1(G)] \supset [D_1(H), D_1(H)] = D_2(H)$．一般に，$D_i(G) \supset D_i(H)$ である．したがって，$D_r(G) = \{e\}$ ならば，$D_r(H) = \{e\}$ であって，H は可解群である．つぎに，N を G の正規部分群とする．G/N において aN と bN の交換子 $[aN, bN] = aba^{-1}b^{-1}N = [a, b]N$ であるから，G/N の交換子群 $D_1(G/N) = D_1(G)N/N$．一般に，$D_i(G/N) = D_i(G)N/N$ である．したがって，$D_r(G) = \{e\}$ ならば，$D_r(G/N) = N$, N は G/N の単位元，となり，G/N は可解群である．

5-2-2 中心列・巾（べき）零群[1)]

ここでも群は有限群とかぎらない．

つぎに，アーベル群と可解群の中間に位置している巾零群について考え

1) 巻末文献 [3],[6],[7],[9] 参照．

る．群 G に対し，$\Gamma_0(G)=G$，$\Gamma_1(G)=[G, G]$，……，$\Gamma_i(G)=[G, \Gamma_{i-1}(G)]$，……，とつぎつぎに G との交換子群をつくる．まず，$\Gamma_1(G)\lhd G$ であるから，$\Gamma_2(G)=[G, \Gamma_1(G)]\lhd G$，$\subset\Gamma_1(G)$．したがって，$\Gamma_3(G)=[G, \Gamma_2(G)]\lhd G$，$\subset\Gamma_2(G)$．一般に，$\Gamma_i(G)$ は $\Gamma_{i-1}(G)$ に含まれる G の正規部分群である．そこで，G の正規部分群列

$$(*)\quad G=\Gamma_0(G)\supset\Gamma_1(G)\supset\cdots\cdots\supset\Gamma_i(G)\supset\cdots\cdots$$

が得られる．ここで，$\Gamma_{i-1}(G)/\Gamma_i(G)$ は $G/\Gamma_i(G)$ の中心に含まれる．なぜなら，G の任意元 x と $\Gamma_{i-1}(G)\ni y$ に対し $[x, y]=xyx^{-1}y^{-1}\in\Gamma_i(G)$ であるから，$xy\Gamma_i(G)=\Gamma_i(G)yx=yx\Gamma_i(G)$ となり，$y\Gamma_i(G)$ は $G/\Gamma_i(G)$ の中心に含まれるから．

［定義］ 上記の正規部分群列 (*) を G の**降中心列**という．降中心列が単位群で終るとき，すなわち，ある r に対し $\Gamma_r(G)=\{e\}$ となるとき，G を**巾零群**という．

アーベル群 G では，$\Gamma_1(G)=[G, G]=\{e\}$ であるから，アーベル群は巾零群である．つぎに，巾零群 G の降中心列は正規鎖であり，各剰余群 $\Gamma_{i-1}(G)/\Gamma_i(G)$ は $G/\Gamma_i(G)$ の中心に含まれているのでアーベル群であるから，降中心列は可換正規鎖である．したがって，巾零群は可解群である．

［定義］ 群 G の正規部分群の列

$$G = G_0 \supset G_1 \supset \cdots\cdots G_i \supset \cdots\cdots \supset G_s = \{e\}$$

は各 G_{i-1}/G_i が G/G_i の中心に含まれるとき，**中心列**という．巾零群の降中心列は中心列である．群 G の中心列において，G_{s-1} は G の中心 Z に含まれる．

［定理 9］ 群 G が中心列 $G=G_0\supset G_1\supset\cdots\cdots\supset G_s=\{e\}$ をもてば，$G_i\supset\Gamma_i(G)$，$i=0, 1, 2, \cdots\cdots, s$．したがって，$G$ は巾零群である．

［系］ 群 G が巾零群であるための必要十分条件は，G が中心列をもつことである．

[定理の証明]　$G_0=G$, $\Gamma_0(G)=G$ より $G_0\supset\Gamma_0(G)$. いま, $G_{i-1}\supset\Gamma_{i-1}(G)$ と仮定する. $G_{i-1}/G_i\subset Z(G/G_i)$ であるから, $G\ni x$, $G_{i-1}\ni y$ に対し, $xyG_i=yxG_i$, $xyx^{-1}y^{-1}\in G_i$ となり, $G_i\supset[G, G_{i-1}]\supset[G, \Gamma_{i-1}(G)]=\Gamma_i(G)$ となる. i に関する帰納法によって, 一般に, $G_i\supset\Gamma_i(G)$ となり, $G_s=\{e\}$ より $\Gamma_s(G)=\{e\}$ となる.

注　群 G の正規部分群の列

$$\{e\}=Z_0\subset Z_1\subset Z_2\subset\cdots\cdots\subset Z_i\subset\cdots\cdots$$

において, Z_1 は G の中心, Z_2 は Z_2/Z_1 が G/Z_1 の中心になるような G の正規部分群, 一般に Z_i/Z_{i-1} は G/Z_{i-1} の中心と一致するとき, この列を G の**昇中心列**という. 群 G が巾零群であるための必要十分条件は, ある自然数 m があって, $Z_m=G$ となることであることがいえる[1]. したがって, 巾零群の昇中心列は中心列である.

例 1.　4次交代群 $\mathfrak{A}_4$ の真の正規部分群は位数4の可換群

$$V=\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

のみであるから, $\mathfrak{A}_4$ の正規部分群列は $\mathfrak{A}_4\supset V\supset\{e\}$ だけである. $\mathfrak{A}_4$ の中心 $Z(\mathfrak{A}_4)=\{e\}$ であるから, $V\not\subset Z(\mathfrak{A}_4)$ で, この列は中心列でない. したがって, $\mathfrak{A}_4$ は巾零群でない. しかし, この列は可換正規鎖であるから, $\mathfrak{A}_4$ は可解群である.

問 1.　3次対称群 $\mathfrak{S}_3$ は可解群であるが, 巾零群でない.

例 2.　つぎの5-2-3項で示すように, p-群は巾零群である. 位数8の4元数群 $\{\pm1, \pm i, \pm j, \pm k\}$ は非アーベル群であるが, 巾零群である.

したがって, アーベル群という概念より巾零群という概念はひろく, 後者より可解群の概念の方がひろいわけである.

可解群の場合と同様に, つぎの2つの定理が成り立つ.

[定理 10]　巾零群の部分群は巾零群である.

[証明]　G を巾零群とし, $G=G_0\supset G_1\supset\cdots\cdots\supset G_s=\{e\}$ を G の中心列とする. $H<G$ のとき, $H_i=H\cap G_i$ とおくと, $H_{i-1}\supset H_i$, $H\triangleright H_i$ である. H の正規部分群列 $H=H_0\supset H_1\supset\cdots\cdots\supset H_s=\{e\}$ は H の中心列である. なぜならば, $[H, H_{i-1}]\subset[G, G_{i-1}]=G_i$, $[H, H_{i-1}]\subset H$ より, $[H, H_{i-1}]\subset H\cap G_i=H_i$ であるから, H の任意元x, H_{i-1} の任意元 y に対し, $xyx^{-1}y^{-1}\in H_i$, $xyH_i=H_iyx=yxH_i$ となるので, $yH_i\in Z(H/H_i)$, したがって $H_{i-1}/H_i\subset Z(H/H_i)$ となるから.

---

1)　巻末文献〔3〕,〔6〕,〔7〕,〔9〕参照.

［定理 11］ 巾零群の準同型像は巾零群である．したがって，とくに巾零群の剰余群は巾零群である．

［証明］ G を巾零群とし，φ を G から群 H の上への準同型とする．N を φ の核とする．G の中心列を $G=G_0\supset G_1\supset\cdots\cdots\supset G_s=\{e\}$ とするとき，$\varphi(G_i)=G_iN/N=H_i$ とおけば，

$$(H)\quad H=H_0\supset H_1\supset\cdots\cdots\supset H_s=\{e\}$$

は H の中心列であることを示そう．まず，G_{i-1}/G_i は G/G_i の中心に含まれる．このことは $[G, G_{i-1}]\subset G_i$ と同値である．したがって，$[\varphi(G), \varphi(G_{i-1})]\subset\varphi(G_i)$，すなわち $[H, H_{i-1}]\subset H_i$ となる．このことは H_{i-1}/H_i が H/H_i の中心に含まれることと同値である．ゆえに上記の（H）は中心列である．

問 2. 可解群の場合とちがって，群 G の正規部分群 N と，G/N が巾零群であっても，G 自身は必ずしも巾零群であるとはかぎらない．（可解群の可換正規鎖を考えてみよ．もしも N と G/N の巾零性から G の巾零性がしたがうとすれば，可解群はすべて巾零群ということになってしまう．）実際に，$G=\mathfrak{S}_3$, $N=\mathfrak{A}_3$ とすれば，$\mathfrak{A}_3$, $\mathfrak{S}_3/\mathfrak{A}_3$ はそれぞれ位数が 3 と 2 であるからアーベル群，したがって巾零群であるが，$\mathfrak{S}_3$ は巾零群ではない．

5-2-3 有限巾零群[1]

［定理 12］ 位数が素数巾 p^n の群，つまり p-群は巾零群である．

［証明］ G を位数が p^n の群とすると，その中心 $Z_1\neq\{e\}$．G/Z_1 も p-群であるから，G/Z_1 が単位群でなければ，G/Z_1 の中心 Z_2/Z_1 は単位群でない．したがって $Z_1\subsetneqq Z_2\triangleleft G$．一般に，$G/Z_{i-1}$ の中心を Z_i/Z_{i-1} とすれば，$Z_{i-1}\subset Z_i\triangleleft G$．$G$ は有限群であるから，いつかは $Z_m=\{G\}$ となる．正規部分群列 $\{e\}=Z_0\subset Z_1\subset\cdots\cdots\subset Z_m=G$ は中心列であるから，G は巾零群である．

注 上記の証明に出てくる中心列は昇中心列である．

例題 1. N は群 G の正規部分群で，G の中心 Z に含まれ，G/N が巡回群ならば，G はアーベル群である．

証明 $G/N=\langle aN\rangle$ とすると，剰余類は a^iN と表される．$N\subset Z$ であるから，G の元は a^ic, $c\in Z$, の形に表される．したがって，G はアーベル群である．

1） 巻末文献〔3〕,〔6〕,〔7〕,〔9〕参照．

この例題から，ただちにつぎのことがいえる．

例題 2． 非可換な p-群 G の中心を Z とすると，G/Z は巡回群ではない．したがって，$|G:Z|\geqq p^2$ である．

例題 3． 位数が 8 の群の構造を決定せよ．

解 G を位数 8 の群とする．

(1) G が位数 8 の元を含めば，G は巡回群である．

(2) すべての元が $x^2=e$ をみたせば，G はアーベル群で，G は不変系が (2, 2, 2) の基本アーベル群である．

(3) G が巡回群でなく，位数 4 の元 a を含むとき，$H=\langle a\rangle$ とおく．H に含まれない元 b をとれば，G は a と b で生成されている．

i) $ab=ba$ であれば，G はアーベル群で，その不変系は (4, 2) である．

ii) $ab\neq ba$ とする．H の指数は 2 であるから，$H\triangleleft G$ で，H の元で位数が 4 のものは a と a^3 だけであるから，$bab^{-1}=a^3$．したがって，もしも $b^2=e$ であれば，G は 4 次の 2 面体群 D_4 と同型である．

iii) もしも，H に含まれない任意元 b について $b^2\neq e$ ならば，b の位数は 4，$H\ni b^2$ の位数は 2 であるから，$b^2=a^2$．したがって，$a^4=e$, $a^2=b^2$, $bab^{-1}=a^3=a^{-1}$ となり，G は 4 元数群と同型である．(p. 63，問題 2 の 11)

さて，群 G が $G=G_1\otimes G_2\otimes\cdots\cdots\otimes G_n$ と直積であるときは，

$$\Gamma_i(G)=\Gamma_i(G_1)\otimes\Gamma_i(G_2)\otimes\cdots\cdots\otimes\Gamma_i(G_n)$$

となるから，G が巾零群であるためには，各直積因子 G_i が巾零群であることが必要十分条件である．

有限群 G に対して，つぎの基本定理を証明するまえに，2 つの補助定理を述べておく．

[補助定理 1] 群 G の部分群 K が p-シロー群 P の正規化群 $N(P)$ を含めば，$N(K)=K$．

[証明] $P\subset N(P)\subset K$ であるから，$N(K)$ の任意元 x に対して，$xPx^{-1}\subset xKx^{-1}=K$ となり，xPx^{-1} も K の p-シロー群である．したがって，$uxPx^{-1}u^{-1}=P$, $u\in K$．したがって，$ux\in N(P)$, $ux\in K$, $x\in K$．ゆえに $N(K)\subset K$．一方，$K\subset N(K)$ であるから，$N(K)=K$．

[補助定理 2] H が巾零群（有限群でも無限群でもよい）G の真の部分群であれば，$H \subsetneqq N(H)$.

[証明] G の降中心列を $G=\Gamma_0 \supset \Gamma_1 \supset \cdots\cdots \supset \Gamma_r=\{e\}$ とする．$G \supsetneqq H$ であるから，$\Gamma_{i-1} \not\subset H$, $\Gamma_i \subset H$ となる Γ_i が存在する．Γ_{i-1} に含まれ，H に含まれない元 x をとる．$H \ni h$ に対し $xhx^{-1}h^{-1} \in \Gamma_i \subset H$ であるから，$xhx^{-1} \in H$. ゆえに $xHx^{-1} \subset H$. また，$x^{-1}hxh^{-1} \in \Gamma_i \subset H$ であるから，上と同様にして，$x^{-1}Hx \subset H$. したがって $H \subset xHx^{-1}$. ゆえに $H=xHx^{-1}$ となって，$x \in N(H)$. $x \notin H$ であるから，$H \subsetneqq N(H)$.

[定理 13] 有限群 G が巾零群であるための必要十分条件は，G がそのシロー群の直積となることである．

[証明] G がそのシロー群の直積になれば，各直積因子であるシロー群は p-群であるから，巾零群であり，したがって，それらの直積である G は巾零群である．逆に G を巾零群とし，$|G|=p_1^{n_1}p_2^{n_2}\cdots\cdots p_r^{n_r}$ を素因数分解とする．p_i の1つを p で表し，G の p-シロー群を P とすれば，補助定理1で，$K=N(P)$ とおくことにより，$N(N(P))=N(P)$. いま，$N(P) \subsetneqq G$ とすれば，補助定理2で $H=N(P)$ とおくことにより，$N(P) \subsetneqq N(N(P))$ となるから，$N(P)=G$ であって，$P \lhd G$. ゆえに G の任意の p_i-シロー群 $P_i \lhd G$. つぎに，積 $P_1P_2\cdots\cdots P_r$ が直積であることを，i に関する帰納法で示す．$i=1$ のときは明白．$i>1$ として，$P_1P_2\cdots\cdots P_{i-1}=P_1 \otimes P_2 \otimes \cdots\cdots \otimes P_{i-1}$ とする．この直積の位数は $p_1^{n_1}\cdots\cdots p_{i-1}^{n_{i-1}}$ で，これは $p_i^{n_i}$ と素であるから，$P_1P_2\cdots\cdots P_{i-1} \cap P_i=\{e\}$ となる．したがって，$P_1P_2\cdots\cdots P_{i-1}P_i=P_1P_2\cdots\cdots P_{i-1} \otimes P_i=P_1 \otimes P_2 \otimes \cdots\cdots \otimes P_{i-1} \otimes P_i$. とくに $i=r$ とすれば，$P_1P_2\cdots\cdots P_r=P_1 \otimes P_2 \otimes \cdots\cdots \otimes P_r$. 位数を比べることによって，$G=P_1 \otimes P_2 \otimes \cdots\cdots \otimes P_r$.

問 1. 有限群 G の位数の各素因子 p に対して p-シロー群が唯一つであれば，G は巾零群である．

問 2. 有限巾零群 G は，その位数の任意の約数 h に対して位数 h の部分群をもつ．

例題 4. 有限群 G が巾零群であるための必要十分条件は，位数が互いに素である任意の2つの元が可換なことである．

証明 a, b を G の，位数が互いに素な2つの元とする．G が巾零群ならば，$G=P_1 \otimes P_2 \otimes \cdots\cdots \otimes P_r$ と，そのシロー群の直積に分解して，a はいくつかの P_i の元の積，b は残りの P_j の元の積に表される．したがって，$ab=ba$ となる．逆に，G の位数が

互いに素な任意の2つの元は可換とする．$|G|=p_1^{n_1}\cdots\cdots p_r^{n_r}$ を素因数分解とし，p_i-シロー群を P_i とすると，仮定によって $i\neq j$ ならば，$P_iP_j=P_jP_i$ であるから，P_1P_2 は部分群であり，その中で，P_1, P_2 は正規部分群で，$P_1\cap P_2=\{e\}$ であるから，$P_1P_2=P_1\otimes P_2$．いま，$P_1\cdots\cdots P_{r-1}=P_1\otimes\cdots\cdots\otimes P_{r-1}$ と仮定すれば，

$$(P_1\cdots\cdots P_{r-1})P_r=P_r(P_1\cdots\cdots P_{r-1}),$$

$$(P_1\cdots\cdots P_{r-1})\cap P_r=\{e\}$$

さらに，$P_1\cdots\cdots P_{r-1}$ と P_r は $P_1\cdots\cdots P_{r-1}P_r$ の正規部分群であるから $(P_1\cdots\cdots P_{r-1})P_r=P_1\cdots\cdots P_{r-1}\otimes P_r=P_1\otimes\cdots\cdots\otimes P_{r-1}\otimes P_r$．位数を比べて $G=P_1\otimes\cdots\cdots\otimes P_r$.

定理13によって，有限巾零群の構造は p-群の構造に帰着される．今までの多くの例題で見たように有限群の構造は，その位数の初等整数論的な性質に関係しているところがある．そういう点からすれば，p-群は最も簡単なものといえるのであるが，現在のところ p-群の構造に関しても十分わかっているとはいえない．

つぎに，簡単なものは位数を割る異なる素数がただ2つのものであるが，つぎの著しい定理が証明されている[1)]．

［定理］（バーンサイド）

位数 $p^\alpha q^\beta$（p, q は異なる素数）の群は可解群である．

現在のところ，この定理の証明には表現論を必要とするので，ここでは結果だけをあげるだけにする．

注　シローの定理は，可解群の場合，ホールによってつぎのように拡張された[2)]．

群 G の位数を g とする．G の部分群 H は，その位数と指数が互いに素であるとき，G の**ホール部分群**という．たとえば，p-シロー群はホール部分群である．

［定理］　G が位数 g の可解群で，$g=mn$, $(m, n)=1$, とすると

(1)　位数 m のホール部分群が少なくとも1つ存在する．

(2)　位数 m の2つのホール部分群は互いに共役である．

(3)　m の約数 m' を位数とする部分群は，位数 m のあるホール部分群に含まれる．

1）巻末文献〔6〕,〔9〕参照．
2）巻末文献〔3〕,〔6〕,〔7〕,〔9〕参照．

注 有限可解群については，つぎの定理が成り立つ[1]．

［定理］ 有限可解群 G は，その位数を $g=p_1^{n_1}p_2^{n_2}\cdots\cdots p_r^{n_r}$（素因数分解）とすると，適当な1組の互いに可換な p_i-シロー群 P_i の積になる：

$$G=P_1P_2\cdots\cdots P_r,\ P_iP_j=P_jP_i\ (i\neq j)$$

逆に，有限群 G が，位数の各素因子に属する，互いに可換なシロー群の積であれば，G は可解群である．

5-3 バーンサイドの定理

バーンサイドは群に関する多くの重要な定理を証明したが，つぎに述べる定理は彼によって証明されたもののうちの1つである．この定理ならびにそれからみちびかれるいくつかの結果は，シロー定理と同様に，位数が小さい群の性質を調べたり，いろいろな位数の群が単純群であるかどうか調べるのに有用である．

バーンサイドの定理を証明するに先立って，まず，移送という概念を説明する．H を群 G の部分群とする．H による G の右分解を．

$$G=x_1H+x_2H+\cdots\cdots+x_nH$$

とする．$G\ni x$ に対して，$x\in x_jH$ のとき，$\phi(x)=x_j$ とおく：$\phi(x)=x_j \Leftrightarrow xH=x_jH$．したがって，$\phi(x)H=xH$．はじめに，つぎのことを示す．

(1) $\phi(xh)=\phi(x)\quad \forall h\in H$

(2) $\phi(a\phi(x))=\phi(ax)\quad \forall a\in G$

(3) $\phi(x)^{-1}x\in H$

証明 (1) $xhH=xH$ であるから，$\phi(xh)=\phi(x)$．

(2) $(a\phi(x))H=a(\phi(x)H)=a(xH)$ であるから，$\phi(a\phi(x))=\phi(ax)$．

(3) $x=\phi(x)h,\ h\in H,$ であるから，$\phi(x)^{-1}x=h\in H$．

いま，G の元 a に対して，

$$(\phi(ax_1)^{-1}ax_1)(\phi(ax_2)^{-1}ax_2)\cdots\cdots(\phi(ax_n)^{-1}ax_n)$$

は，(3)によって，H の元で，これの属する $H/D(H)$，$D(H)$ は H の交換

1） 巻末文献〔7〕参照．

子群，の剰余類を $V_{G\to H}(a)$ で表し，a の G から H への移送という．

(4)　$a \longmapsto V_{G\to H}(a)$ は G からアーベル群 $H/D(H)$ の中への準同型である．

証明　G の2つの元 a, b に対して，

$$V_{G\to H}(ab) = \prod_{i=1}^{n}(\phi(abx_i)^{-1}abx_i)D(H)$$

$$= \prod_{i=1}^{n}\{\phi(abx_i)^{-1}a\phi(bx_i)\phi(bx_i)^{-1}bx_i\}D(H)$$

$$= \prod_{i=1}^{n}(\phi(abx_i)^{-1}a\phi(bx_i))\prod_{i=1}^{n}(\phi(bx_i)^{-1}bx_i)D(H)$$

さて，i が1から n まで動くとき，$\phi(bx_i)H=bx_iH$ は，$x_1H, x_2H, \cdots\cdots, x_nH$ 全体を動くから，$\phi(bx_i)$ は，$x_1, x_2, \cdots\cdots, x_n$ 全体を1わたり動く．つぎに(2)より，$\phi(abx_i)=\phi(a\phi(bx_i))$ であるから，

$$\prod_{i=1}^{n}(\phi(abx_i)^{-1}a\phi(bx_i))D(H) = V_{G\to H}(a)$$

したがって，$V_{G\to H}(ab)=V_{G\to H}(a)V_{G\to H}(b)$.

(5)　$V_{G\to H}(a)$ は代表系 $\{x_i\}$ のとり方に無関係である．

証明　いま，x_iH から別の代表 x_i' を選べば，$x_i'=x_ih_i$, $h_i\in H$. $G\ni x$ に対して $x\in x_i'H$ のとき $\phi'(x)=x_i'$ とおき，$V'_{G\to H}(a)=\prod_{i=1}^{n}(\phi'(ax_i')^{-1}\ ax_i')D(H)$ と定義する．いま，$ax_i=x_{\sigma(i)}c_i$, $c_i\in H$, とすれば，$\phi(ax_i)=x_{\sigma(i)}$, $\phi(ax_i)^{-1}ax_i=x_{\sigma(i)}{}^{-1}x_{\sigma(i)}c_i=c_i$ となる．つぎに，$ax_i'=ax_ih_i=x_{\sigma(i)}c_ih_i=x'_{\sigma(i)}h_{\sigma(i)}{}^{-1}c_ih_i$, ここで $h_{\sigma(i)}, c_i, h_i\in H$ である．したがって，$\phi'(ax_i')^{-1}ax_i'=x'_{\sigma(i)}{}^{-1}ax_i'=h_{\sigma(i)}{}^{-1}c_ih_i$. いま，$i$ が1から n まで動くと，$\sigma(i)$ も全体として，1から n の間を1わたり動くから，

$$V'_{G\to H}(a) = \prod_{i=1}^{n}(h_{\sigma(i)}{}^{-1}c_ih_i)D(H)$$

$$= (\prod_{i=1}^{n}h_{\sigma(i)}{}^{-1}\prod_{i=1}^{n}c_i\prod_{i=1}^{n}h_i)D(H)\quad (H/D(H) \text{ がアーベル群ゆえ})$$

$$= (\prod_{i=1}^{n}c_i)D(H) = \prod_{i=1}^{n}(\phi(ax_i)^{-1}ax_i)D(H) = V_{G\to H}(a)$$

準同型 $V_{G\to H}$ の核を K とすれば，$G/K\cong V_{G\to H}(G)$ で，右辺はアーベル群 $H/D(H)$ の部分群であるから，アーベル群である．したがって，K は G の交換子群を含む．以上まとめて，

[定理 14] 群 G から部分群 H への移送 $V_{G\to H}$ は，H を法とする右剰余類の代表元のとり方に無関係に定義され，G からアーベル群 $H/D(H)$ の中への準同型である．この準同型の核は G の交換子群を含む．

移送 $V_{G\to H}$ は，H からアーベル群 $H/D(H)$ の上への自然な準同型を，G 全体に拡げようとするものであって，整数論においても有用である．

いま，G の元 a に対して，$\Delta=\{x_iH,\ i=1, 2, 3, \cdots\cdots, n\}$ から Δ 自身への写像 $\pi(a)$ を $\pi(a): x_iH \longmapsto ax_iH$ によって定義する．$ax_iH=ax_jH$ ならば $x_iH=x_jH$ であるから，$\pi(a)$ は Δ の上の1対1写像，つまり置換である．$\pi(ab)=\pi(a)\pi(b)$ であるから，$\pi: a\longmapsto \pi(a)$ によって，G は n 次対称群 $\mathfrak{S}_n$ の中に準同型にうつされる（この準同型 π を G の部分群 H による**置換表現**[1] という）．さて，置換 $\pi(a)$ を共通の文字を含まない巡回置換の，一項からなる置換も含めた積に分解して，

$\pi(a)=(x_1H, \cdots\cdots, a^{f_1-1}x_1H)\cdots\cdots(x_tH, \cdots\cdots, a^{f_t-1}x_tH)$ とすれば，$f_1+f_2+\cdots\cdots+f_t=|G:H|$ であり，H を法とした右剰余類の代表系として $\{x_1, \cdots\cdots, a^{f_1-1}x_1, \cdots\cdots, x_t, \cdots\cdots, a^{f_t-1}x_t\}$ をとることができる．$\phi(a^jx_i)$ は，$0<j<f_i$ のとき a^jx_i，$j=f_i$ のとき x_i であるから，$\phi(a(a^{j-1}x_i))^{-1}a(a^{j-1}x_i)$ は $0<j<f_i$ のとき e，$j=f_i$ のとき $x_i^{-1}a^{f_i}x_i$ である．$x_i^{-1}a^{f_i}x_i\in H$ であり，このとき $V_{G\to H}(a)=\prod_{i=1}^{t} x_i^{-1}a^{f_i}x_iD(H)$ である．

以上で準備は終ったので，いよいよ，つぎの定理を証明しよう．

[定理 15] **（バーンサイドの定理**[2]**）**

群 G の p-シロー群 P がアーベル群で，その正規化群 $N(P)$ の中心に入るなら，G は $MP=G,\ M\cap P=\{e\}$ であるような正規部分群 M を含む（$G/M\cong P$ であるような正規部分群 M を含むといってもよい）．

[証明] 仮定から $D(P)=(e)$ であるから，$V_{G\to P}$ は G から P への準同型である．そこで $V_{G\to P}=P$ がいえれば，$V_{G\to P}$ の核を M とするとき，$M\lhd G$ で $G/M\cong P$ となって，定理は証明されたことになる．

1） 付録5参照.
2） 巻末文献〔3〕,〔6〕,〔7〕,〔9〕参照.

$V_{G\to P}$ を V で表す．$P\ni a$ に対して $V(a)$ を先の式で計算すれば，

$$V(a)=(x_1^{-1}a^{f_1}x_1)\cdots\cdots(x_t^{-1}a^{f_t}x_t)$$

a^{f_i} と $x_i^{-1}a^{f_i}x_i$ はともにアーベル群 P の元で，G で共役であるから，p. 103，例題1より，$N(P)$ で共役．したがって，仮定により，$a^{f_i}=x_i^{-1}a^{f_i}x_i$ となる．したがって，$g'=|G:P|$ とすると，$V(a)=a^{f_1}a^{f_2}\cdots\cdots a^{f_t}=a^{g'}$．さて $(g',p)=1$ であるから，a が P 全体を動けば，$a^{g'}$ も P 全体を動くので，$V(P)=P$ であり，もちろん $V(G)=P$ となる．

[系]　群 G の p-シロー群 P がアーベル群で，$N(P)=P$ であれば，G は $MP=G$, $M\cap P=\{e\}$ であるような正規部分群 M を含む．

注　P が $N(P)$ の中心 $Z_{N(P)}$ に含まれる $\Leftrightarrow$ P の中心化群 $Z(P)$ は $N(P)$ と一致する．$\Longrightarrow$ をいう．$\forall a\in P\subset Z_{N(P)}$, $na=an$, $\forall n\in N(P)$，ゆえに $N(P)\subset Z(P)$．一般に，$Z(P)\subset N(P)$ であるから，$Z(P)=N(P)$．$\Longleftarrow$ を示す．$\forall n\in N(P)=Z(P)$, $na=an$, $\forall a\in P$．したがって $P\subset Z_{N(P)}$．

例題 1.　位数が $3^3\cdot 13$ の群 G は単純群でない．

証明　G が単純群だとすると，13-シロー群 P の共役は 27 個あるから，$|G:N(P)|=27$．したがって $P=N(P)$．P は巡回群であるから，上の系から，G は真の正規部分群を含み，矛盾を生じる．

問 1.　位数が 400 の群は単純群でない．

例題 2.　群 G の p-シロー群 P に対し，$N(P)=Z(P)$ であれば，G の交換子群 $D(G)$ の位数は p で割り切れない．

証明　G は $MP=G$, $M\cap P=\{e\}$ である正規部分群 M を含み，$G/M\cong P$．P はアーベル群であるから（上の注），$M\supset D(G)$．p は M の位数を割り切らないから，p は $D(G)$ の位数を割り切らない．

以下定理 15 のいくつかの応用を示す[1]．

[定理 16]　群 G の p-シロー群 P がアーベル群で，$N(P)/P$ の位数が P の自己同型群 $A(P)$ の位数と互いに素であれば，G は $MP=G$, $M\cap P=\{e\}$ であるような正規部分群 M を含む．

[証明]　$P\triangleleft N(P)$ であるから，$N(P)$ の元 a により，$x\longmapsto axa^{-1}$ という P の

1）巻末文献〔10〕参照．

自己同型 $\sigma(a)$ が引き起こされる．a の属する法 P の剰余類の位数を m とすれば，$a^m \in P$, $\sigma(a)^m = \sigma(a^m)$ は P の恒等写像である．仮定によって，m は $A(P)$ の位数と互いに素であるから，$\sigma = I$. したがって，$axa^{-1} = x \quad \forall x \in P$. ゆえに P は $N(P)$ の中心に含まれる．したがって，バーンサイドの定理によって，G は $MP=G$, $M \cap P = \{e\}$ であるような正規部分群 M を含む．

例題 3. 位数が 396 の群 G は単純群でない．

証明 G が単純群だとすると，11-シロー群 P の共役の個数は 12. したがって，$|N(P)| = 33$. $|N(P)/P| = 3$ は位数 11 の群 P の自己同型群の位数 φ (11)=10 と互いに素であるから，G は真の正規部分群を含むことになって，矛盾を生じる．

問 2. 位数が $2^3 \cdot 3 \cdot 7 \cdot 23$ の群は単純群でない．

[系 1] 素数 p は，群 G の位数 g の素因数で，$(g, p-1)=1$ とする．G の p-シロー群 P が巡回群であれば，G は $MP=G$, $M \cap P = \{e\}$ であるような正規部分群 M を含む．

[証明] $|P| = p^r$ とすれば，巡回群 P の自己同型群の位数は $\varphi(p^r) = p^{r-1}(p-1)$. $N(P)/P$ の位数は p と素で，$(g, p-1)=1$ であるから，$N(P)/P$ の位数は $p^{r-1}(p-1)$ と素である．したがって，定理 16 により，$\exists M \triangleleft G$, $G=MP$, $M \cap P = \{e\}$.

[系 2] 群 G の位数の最小の素因数を p とする．G の p-シロー群 P が巡回群であれば，G は $MP=G$, $M \cap P = \{e\}$ である正規部分群 M を含む．

[証明] このとき，$(|G|, p-1)=1$ であるから．

[定理 17] 群 G の位数を g とする．G のある部分集合 K の共役の個数 n が $n \geqq 2$ で，$g \nmid n!$ ならば，G は単純群ではない．

[証明] K の共役を $K=K_1, K_2, \cdots\cdots, K_n$ とする．G の元 a に対し，

$$\pi(a) = \begin{pmatrix} K_1 & K_2 & \cdots\cdots & K_n \\ aK_1a^{-1} & aK_2a^{-1} & \cdots\cdots & aK_na^{-1} \end{pmatrix}$$

とすると，$\pi : a \longmapsto \pi(a)$ は G から n 次対称群 $\mathfrak{S}_n$ への自明でない準同型である．G が単純群ならば，π の核は $\{e\}$, π は同型であって，$\pi(G)$ は $\mathfrak{S}_n$ の部分群となり，$g | n!$. 対偶をとって，$g \nmid n!$ ならば，G は単純群でない．

[系] 群 G の位数を g とする．G のある真の部分群 H の指数 m につ

いて，$g \nmid m!$ であれば，G は単純群でない．

［証明］　H の共役の個数 $n=|G:N(H)|$ は指数 $m=|G:H|$ の約数であるから，$g \nmid m!$ であれば $g \nmid n!$.

例題 4.　位数 300 の群 G は単純群でない．

証明　G の 5-シロー群 P の共役の個数 n_5 は 12 の約数で，$1+5k$ の形をしているから，1 か 6．G が単純群だとすると，$n_5=6$ であるが，$300 \nmid 6!$ であるから，これは矛盾である．

問 3.　群 G は，その位数 g がつぎの各場合，単純群でない．

$g=36, 72, 2^2\cdot 3^n(n \geqq 2), 2^3\cdot 7^n(n \geqq 2), 108, 324, 600, 648, 900, 3^3\cdot 5\cdot 7$

例題 5.　位数 144 の群 G は単純群でない．

証明　G が単純群だとする．G の 3-シロー群 P の共役の個数 n_3 は 4 か 16．$n_3=16$ とすれば，$N(P)=P$ で，$|P|=3^2$ であるから，P はアーベル群．定理 15 の系から，G は真の正規部分群を含むことになり，矛盾を生じる．したがって，$n_3=4$ でなくてはならない．しかし，$144 \nmid 4!$ で，G は単純群でないということになって，これも矛盾である．

問 4.　位数が 540 の群は単純群ではない．

［定理 18］　単純群の位数は 12 で割り切れるか，位数 g の最小の素因数 p の 3 乗で割り切れる．

［証明］　(1)　$g \not\equiv 0 \pmod{p^2}$ とすれば，G の p-シロー群 P の位数は p であるから，P は巡回群である．p は g の最小素因数であるから，$(g, p-1)=1$．したがって，定理 16 の系 1 から，G は真の正規部分群を含むことになるので，$g \equiv 0 \pmod{p^2}$ でなくてはならない．

(2)　$g \equiv 0 \pmod{p^2}$, $\not\equiv 0 \pmod{p^3}$ とする．このとき P の位数は p^2 である．はじめに P が巡回群だとすると，定理 16 系 2 によって，G は真の正規部分群を含むことになるから，$p^3|g$ でなくてはならない．つぎに，P が不変系が (p, p) の基本アーベル群とすると，P の自己同型群の位数 $l=(p^2-1)(p^2-p)=p(p-1)^2(p+1)$ である（p. 91，例題 4）．したがって，$p \neq 2$ のとき，l は $N(P)/P$ の位数と素であるから，定理 16 によって，G は真の正規部分群を含むことになるから，$p^3|g$ でなくてはならない．また $p=2$ のときは，かりに $3 \nmid g$ であれば，l と $N(P)/P$ の位数は素になり，やはり G は真の正規部分群を含むことになるから，$3|g$ でなくてはならない．したがって，$2^2|g$, $3|g$ より，$12|g$ である．

例題 6. 位数が 60 の単純群は 5 次交代群 $\mathfrak{A}_5$ に同型である.

証明 G を位数 60 の単純群とする. G の 2-シロー群 P の共役の個数 n_2 は 3 か 5 か 15 である. $n_2=15$ とすれば, $N(P)=P$ で, P は位数 4 の群であるから, アーベル群である. したがって, G の真の正規部分群を含むことになるから, $n_2 \neq 15$. つぎに $n_2=3$ とする. このとき, P が巡回群ならば, 定理 16 系 2 によって, G は真の正規部分群を含むことになるから, P は巡回群でなく, 不変系が $(2, 2)$ の基本アーベル群でなくてはならない. このとき, P の自己同型群の位数 $l=(2^2-1)(2^2-2)=6$ は, $N(P)/P$ の位数 5 と互いに素であるから, 定理 16 より, G は真の正規部分群を含むことになる. したがって, $n_2 \neq 3$ で, 結局, $n_2=5$. いま $N=N(P)$ とおく. G の N を法とした右分解を $G=x_1N+x_2N+\cdots\cdots+x_5N$ とし, $\varDelta=\{x_1N, x_2N, \cdots\cdots, x_5N\}$ とおく. 先の移送のところで述べたように, G の元 a に対して, $\pi(a): x_iN \longmapsto ax_iN$ という $\varDelta$ から $\varDelta$ への写像を考える. $ax_iN=ax_jN$ なら $x_iN=x_jN$ であるから, $\pi(a)$ は $\varDelta$ の上の置換で, $\pi(ab)=\pi(a)\pi(b)$ であるから, $\pi: a \longmapsto \pi(a)$ は G から $\mathfrak{S}_5$ への準同型である (π は G の N による置換表現である. p. 117). G は単純群であるから, π の核を K とすれば, $K=\{e\}$ で, π は同型である. $\pi(G)$ は $\mathfrak{S}_5$ の部分群で, 位数が 60 であるから, $\pi(G)$ は $\mathfrak{A}_5$ であり, 結局 $G \cong \pi(G)=\mathfrak{A}_5$.

問 5. 上記の証明で, π の核 K は N に含まれる最大の正規部分群である.

以下, 位数が $p^m q^n$ (p, q は異なる素数) の群は可解群であるという定理 (バーンサイド) を仮定する.

例題 7. 位数が 60 より小さい群は可解群である.

証明 位数が素数巾か $p^m q^n$ (p, q は素数, $p \neq q$) の群は可解群であるから, 位数が $2\times3\times5=30$ の群 G と, $2\times3\times7=42$ の群 G について調べればよい. いずれの群にしても, $2^3 \nmid 30$, $2^3 \nmid 42$, また, $12 \nmid 30$, $12 \nmid 42$ であるから, 単純群でない. したがって, G は真の正規部分群 G_1 をもつ. $|G_1|=$素数 r であれば, $|G/G_1|=pq$ (p, q は異なる素数) であって, G_1, G/G_1 ともに可解群であるから, G も可解群である. $|G_1|=pq$ であれば, $|G/G_1|=r$ であるから, G_1, G/G_1 ともに可解群であるから, G も可解群である.

例題 8. 位数が 60 より大きく, 120 より小さい群は可解群である.

証明 $60<|G|<120$ のとき, G が単純群でないことをいえばよい. なぜなら, そのとき G は正規部分群 G_1 をもつが, $|G_1|$, $|G/G_1|$ のいずれも 60 より小さいから,

G_1, G/G_1 は可解群で，したがって，G 自身可解群であるから.

さて，単純群になり得る群の位数 $m<120$ はつぎのとおりである.

i） $8|m$, $m\neq 2^r$, $2^r p^s$. しかし，$8\times n$, $n<15$ では，そのような m は存在しない.

ii） $12|m$, $m\neq 2^r 3^s$. $60=12\times 5$ を除いては $84=12\times 7$ だけである．G を位数 84 の群とし，7-シロー群を P とする．P の共役の個数は，12 の約数で，しかも $1+7k$ の形をしているから，1 である．したがって，$P\lhd G$ であり，G は単純群でない.

iii） $3^3|m$, $m\neq 3^r p^s$. このような m は存在しない.

上の結果から，5 次交代群 $\mathfrak{A}_5$ が位数が最小の単純群であることがわかった．また位数が 120 になると，5 次の対称群 $\mathfrak{S}_5$，5 次の交代群 $\mathfrak{A}_5$ と位数 2 の巡回群の直積，および，つぎに述べる群 SL (2, 5) の 3 つの非可解群が存在する．$\mathfrak{S}_5$ は先に述べたように非可解群である．$\mathfrak{A}_5\otimes\langle a\rangle$, $\langle a\rangle$ は位数 2 の巡回群，も非可解群である．かりに可解群とすれば，部分群 $\mathfrak{A}_5$ が可解群となるからである．$SL(2, 5)$ が非可解であることは，かりに可解とすれば，その正規部分群 $C=\{E, -E\}$ とともに，$SL(2, 5)/C=LF(2, 5)$ が可解でなくてはならないが，$LF(2, 5)$ は単純群で，非可解であるからである.

5-4 単純群の例[1]

$n\geqq 5$ のとき，n 次交代群 $\mathfrak{A}_n$ は単純群であることは，p. 97，例題 4 で述べた．その他に単純群の例として，つぎに述べる 1 次分数変換群がある.

いま，p を素数とし，K を p 個の元からなる体 $\boldsymbol{Z}_p$ とする．K 上の一般 1 次変換群 $GL(2, K)$，つまり K の元を成分とする 2 次の正則行列のつくる群を $GL(2, p)$ で表し，$GL(2, p)$ の中で行列式が 1 である行列のつくる特殊 1 次変換群を $SL(2, p)$ で表す[2]．いま，

$$C=\{\lambda E, \lambda\in K, \lambda^2=1\}=\{E, -E\}$$

とおくと，C は $SL(2, p)$ の中心である．($\boldsymbol{Z}_p$ の乗法群は巡回群で，$\lambda^2=1$ となる λ は 1 と -1 の 2 つしかない)．C が中心に含まれることは明白．A

1） 巻末文献〔3〕の第 I 巻，〔10〕.
2） 付録 7 参照.

$=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$が中心の元ならば，とくに$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, と可換なことから，$a=d$, $b=c=0$ がみちびかれるからである．

注 $p=2$ のときは $C=\{E\}$ である．

$GL(2, p)$ は $K=\boldsymbol{Z}_p$ 上の 2 次元ベクトル空間[1]の 1 対 1 の 1 次変換全体のつくる群とみなされる．いま，つぎの等式を示す．

$$|GL(2, p)| = (p^2 - 1)(p^2 - p) = p(p - 1)^2(p + 1)$$

$GL(2, p)$ の行列は，

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}, \quad a_1b_2 - a_2b_1 \neq 0, \qquad \text{つまり } (a_2, b_2) \neq \lambda(a_1, b_1)$$

まず，(a_1, b_1) の選び方は，$(0, 0)$ を取れないことに注意すれば，p^2-1 通りある．1 つの (a_1, b_1) に対し，(a_2, b_2) の選び方は，$(\lambda a_1, \lambda b_1)$ の形のものはとれないから，p^2-p 通りある．したがって，$|GL(2, p)|=(p^2-1)(p^2-p)$.

つぎに，$GL(2, p)\ni A \longmapsto$ 行列式 $|A|\in\boldsymbol{Z}_p{}^*$ は上への準同型で，その核が $SL(2, p)$ であるから，

$$|GL(2, p) : SL(2, p)| = |\boldsymbol{Z}_p{}^*| = p - 1$$

ゆえに $|SL(2, p)| = p(p - 1)(p + 1)$.

剰余群 $SL(2, p)/C$ を $LF(2, p)$ で表し，これを 1 次**分数変換群**という．$p\neq2$ ならば $|LF(2, p)|=p(p^2-1)/2$.

$p=2$ のとき，$GL(2, 2)=SL(2, 2)$ で，中心 $C=\{E\}$ であるから，$SL(2,2)=LF(2, 2)$ であり，$LF(2, 2)$ は位数 6 の非可換群であるから，$SL(2, 2)=LF(2, 2)\cong\mathfrak{S}_3$.

$p=3$ のときは，$SL(2, 3)$ の位数は $3\cdot2\cdot4=24$ であり，中心 $C=\{E, -E\}$ であるから，$LF(2, 3)$ の位数は 12 である．ところで，$LF(2, 3)$ の中心は単位類だけからなる．それをいうには，$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$が中心に属する剰余類の行

1) 付録 7 参照.

列とすれば，

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(\pm E)$$

であるから，$a=\pm d$, $b=\mp c$（複号同順）であり，また，

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(\pm E)$$

でなくてはならないが，右辺で $-E$ はとれなくて，$+E$ としたとき，$c=0$ となるから，結局 $b=c=0$, $a=\pm d$. そこで $ad=\pm a^2\equiv 1 \pmod 3$ であるが，$-a^2\equiv 1 \pmod 3$ は成り立たないから，$a=d$, $a^2\equiv 1 \pmod 3$ より，$a\equiv 1$ または $\equiv -1 \pmod 3$ となる．

［補題］ 位数 12 の群 G の中心が位数 2 の元を含まないならば，$G\cong\mathfrak{A}_4$.

証明 G の 3-シロー群 $P=\langle x\rangle$ である．まず $P\lhd G$ でないことを示す．かりに $P\lhd G$ とすれば，G の 2-シロー群を Q とするとき，$G=PQ$. G の任意の元 a に対し $axa^{-1}\in P$ であるから，x の共役元はたかだか x と x^2 の 2 つしかなく，$|G:Z(x)|\leqq 2$. いま $G=Z(x)$ とすると，アーベル群 Q の中の位数 2 の元 y は，$yx=xy$ をみたすから，G の中心に属し，仮定に反する．つぎに $|G:Z(x)|=2$ とすると，$Z(x)$ の位数は 6 で，P はその正規な 3-シロー群であるから，$Z(x)$ の，P に入っていない元 z の位数は 6 か 2 である．z の位数が 6 ならば，z^3 の位数は 2 で，$z^3x=xz^3$. いずれにしても G の位数 2 の元 y で $yx=xy$ となるものがある．y はアーベル群 Q に入っている．y は G の中心に属し，仮定に反する．したがって，P は G の正規部分群でない．さて，$|G:P|=4$ であるから，P による G の置換表現 ϕ によって，G は $\mathfrak{S}_4$ に準同型にうつされる．ϕ の核は P に含まれる G の最大の正規部分群であるから，それは単位群である．したがって，ϕ は同型で，$\phi(G)$ は $\mathfrak{S}_4$ の位数 12 の部分群である．そのような部分群は $\mathfrak{A}_4$ しかないから，結局，$G\cong\phi(G)=\mathfrak{A}_4$.

したがって，$L(2,3)\cong\mathfrak{A}_4$ である．

上に示したように，$LF(2,2)$，$LF(2,3)$ は非単純な可解群であるが，

［定理 19］ $p=2$ および $p=3$ の場合を除いて，$LF(2,p)$ は単純群である．

［証明］ はじめに $SL(2,p)$ の生成元を求める．$E(i,j;\lambda)$, $i\neq j$, は対角線には

1がならび，i 行 j 列のところは $K\ni\lambda\neq 0$，その他は0である行列とする．$E(i, j; \lambda)^{-1}=E(i, j; -\lambda)$ である．$SL(2, p)\ni A=(a_{ij})$ で，$a_{12}=0$ ならば，$a_{11}\neq 0$ であるから，$A'=AE(1, 2; \lambda)$ とおくと，A' の (1, 2) 成分は0でない．いま $a_{12}\neq 0$ と仮定する．$A''=AE(2, 1; \lambda)$ とおくと，(1, 1) 成分は $a_{11}+\lambda a_{12}$ であるから，λ を適当にとって，A'' の (1, 1) 要素を1とする．したがって，A からはじめてその右から $E(1, 2; \lambda)$，左から $E(2, 1; \mu)$ を適当にかけると，A は対角線以外は0で，対角線上に1と ν が並んだ形になる．ところが $|A|=1$，$|E(i, j; \lambda)|=1$ であるから，$\nu=1$ であって，最後の行列は E である．$E(i, j; \lambda)^{-1}=E(i, j; -\lambda)$ であるから，A はいくつかの $E(i, j; \lambda)$ の積で表される．

以下，$G=LF(2, p)$ とおく．G は $E(i, j; \lambda)C$ で生成される．

$$\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}\begin{pmatrix}1 & \mu\\ 0 & 1\end{pmatrix}\begin{pmatrix}\lambda^{-1} & 0\\ 0 & \lambda\end{pmatrix}\begin{pmatrix}1 & -\mu\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & \mu(\lambda^2-1)\\ 0 & 1\end{pmatrix}$$

で，$p>3$ であるから，$\lambda\neq 0$，$\lambda^2\neq 1$ となる λ が存在するので，任意の $E(1, 2; \lambda)$は交換子である．同様に，$E(2, 1; \lambda)$ も交換子であるから，$D(G)=G$ である．

いま，K 上のゼロベクトル $\mathbf{0}=(0,0)$ 以外の2次元ベクトル全体を V^* とし，$\boldsymbol{a}\sim\boldsymbol{b} \iff \boldsymbol{b}=\lambda\boldsymbol{a}$，$\lambda\in K$，とすれば，$V^*$ は類別される．V^* のベクトルは p^2-1 個あり，各類に $p-1$ 個のベクトルが含まれるから，類の個数は $(p^2-1)/(p-1)=p+1$ である．これらの類を $\boldsymbol{C}_i$, $i=1,2\cdots\cdots$, $t=p+1$ とする．$SL(2,p)$ の元 A, A' について，$A\sim A' \pmod{C} \iff A=\lambda A'$, $\lambda\in K$, $\lambda^2=1$，であるから，$\boldsymbol{a}_i\in\boldsymbol{C}_i$ について，$\boldsymbol{a}_iA\in\boldsymbol{C}_j$ のとき，$\boldsymbol{a}_iA'\in\boldsymbol{C}_j$ であり，また $\boldsymbol{a}_i'\in\boldsymbol{C}_i$ ならば，$\boldsymbol{a}_i'A\in\boldsymbol{C}_j$ となるから，G の各類は $p+1$ 個の $\boldsymbol{C}_1$, $\boldsymbol{C}_2$, ……, $\boldsymbol{C}_{p+1}$ の上の置換を引き起こす：$LF(2, p)\ni a$ のとき a から1つの行列 A をとって $\boldsymbol{C}_ia=\{\boldsymbol{a}_iA|\boldsymbol{a}_i\in\boldsymbol{C}_i\}$．こうして，$G$ と対応する置換のつくる群は同型である（置換の積を，左側を先にほどこすと定義する）．

いま，$H=\left\{A|A=\begin{pmatrix}a & 0\\ c & d\end{pmatrix}\in SL(2, p),\ ad=1\right\}$

とおく．$\varphi(A)=a$ により H は$K^*=\boldsymbol{Z}_p^*$ の上に準同型にうつり，φ の核は

$$N_0=\left\{B|B=\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix},\ c\in K\right\}$$

である．$\tilde{H}=HC/C$，$\tilde{N}_0=N_0C/C$ とおく．N_0 はアーベル群であるから，$\tilde{N}_0$ もアー

ベル群である．いま $N\neq\{e\}$ を G の正規部分群とすると，あとで示すように，$N\tilde{H}=G$ となる．$N_0\triangleleft H$ であるから，$\tilde{N}_0\triangleleft\tilde{H}$ であり，したがって，$N\tilde{N}_0\triangleleft G$. なぜなら，$N\tilde{H}$ の任意の元 nh, $n\in N$, $h\in\tilde{H}$, に対して，$nhN\tilde{H}_0=Nnh\tilde{N}_0=N\tilde{N}_0h=\tilde{N}_0Nh=\tilde{N}_0Nnh=N\tilde{N}_0nh$ であるから．つぎに，$E(2,1;\lambda)\in N_0$ であるから，$E(2,1;\lambda)C\in N\tilde{N}_0$. $\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}1&0\\\lambda&1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}1&-\lambda\\0&1\end{pmatrix}$ であるから，$N\tilde{N}_0$ はすべての $E(i,j;\lambda)C$ を含むことになって，$N\tilde{N}_0=G$. したがって，$G/N=N\tilde{N}_0/N\cong\tilde{N}_0/N\cap\tilde{N}_0$. $\tilde{N}_0$ はアーベル群であるから，G/N はアーベル群で，$N\supset D(G)=G$, ゆえに $N=G$. したがって G は単純である．

最後に，残っている $N\tilde{H}=G$ を示す．$SL(2,p)$ の中にはベクトル $(1,0)$ を $\boldsymbol{a}=(\alpha_1,\alpha_2)\neq(0,0)$ にうつす行列が存在する．それには $\boldsymbol{b}=(\beta_1,\beta_2)\neq\lambda\boldsymbol{a}$, $\neq(0,0)$ をとり，行列 $A=\begin{pmatrix}\alpha_1&\alpha_2\\\beta_1&\beta_2\end{pmatrix}$ をつくればよい．$|A|=\mu\neq0$ が 1 でなければ，$\boldsymbol{b}$ の代りに $\mu^{-1}\boldsymbol{b}$ をとればよい．いま $(1,0)$ の属する類を $\boldsymbol{C}_1$ とすれば，先の H は $\boldsymbol{C}_1$ を動かさない $SL(2,p)$ の行列全体である．いま $SL(2,p)\ni B$ によって，$(1,0)B\in\boldsymbol{C}_i$ であれば，$B^{-1}HB$ は $\boldsymbol{C}_i$ を動かさない $SL(2,p)$ の行列全体である．したがって，B の属する剰余類を $b\in G$ とすれば，$\bigcap b^{-1}\tilde{H}b$, ここで b は G 全体を動く，はすべての $\boldsymbol{C}_i$ を動かさないから，この共通部分は $\{e\}$. したがって，$N\triangleleft G$ であるから，$N\not\subset\tilde{H}$. したがって，$a\in N$, $a\notin\tilde{H}$ という元 a が存在する．いま，$\boldsymbol{C}_1a=\boldsymbol{C}_2$ とする．任意の $\boldsymbol{C}_j(j\geqq2)$ に対し，$\boldsymbol{C}_2$ を $\boldsymbol{C}_j$ にうつす $\tilde{H}$ の元が存在する．なぜならば，$\boldsymbol{C}_2$ から代表 $(\alpha,1)$, $\boldsymbol{C}_j$ から代表 $(\beta,1)$ をとると，

$$(\alpha,1)\begin{pmatrix}1&0\\\beta-\alpha&1\end{pmatrix}=(\beta,1)$$

であるから．そこで，$\tilde{H}\ni h_j$, $\boldsymbol{C}_2h_j=\boldsymbol{C}_j$ とすると，$\boldsymbol{C}_1h_j^{-1}ah_j=\boldsymbol{C}_1ah_j=\boldsymbol{C}_2h_j=\boldsymbol{C}_j$ であり，この $h_j^{-1}ah_j=g_j\in N$. いま，g を G の任意の元とし，$\boldsymbol{C}_1g=\boldsymbol{C}_j$ であれば，$\boldsymbol{C}_1gg_j^{-1}=\boldsymbol{C}_jg_j-1=\boldsymbol{C}_1$ であるから，$gg_j^{-1}\in\tilde{H}$, $g\in\tilde{H}N=N\tilde{H}$. ゆえに $G=N\tilde{H}$.

注　実際には，体 $\boldsymbol{Z}_p$ の代りに K として，任意の可換体をとって，K 上の n 次特殊1次変換群 $SL(n,K)$ のその中心 $C=\{\lambda E,\lambda^n=1\}$ による剰余群 $LF(n,K)$ をつくれば，これは単純群であることがわかっている[1].

$LF(n,p)$ の位数は，

1） 巻末文献〔3〕参照．

$$\frac{p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\cdots\cdots(p^2-1)}{(n,\ p-1)}$$ [1]

n, p の小さいとき，$L(n, p)$ の位数を求めると，

n \ p	2	3	5	7	11	13
2	—	—	$2^2\cdot3\cdot5=60$	$2^3\cdot3\cdot7$ $=168$	$2^3\cdot3\cdot5\cdot11$ $=660$	$2^2\cdot3\cdot7\cdot13$ $=1092$
3	$2^3\cdot3\cdot7$ $=168$	$2^4\cdot3^2\cdot13$ $=5616$	$2^5\cdot3\cdot5^3\cdot31$ $=37200$	$2^5\cdot3^2\cdot7^3\cdot19$ $=1876896$	$2^4\cdot3\cdot5^2\cdot7\cdot$ $11^3\cdot19$	$2^4\cdot3^2\cdot7\cdot$ $13^3\cdot61$
4	$2^6\cdot3^2\cdot5\cdot7$ $=20160$	$2^7\cdot3^6\cdot5\cdot13$ $=6065280$				

単純群の位数で1000より小さいものは60, 168, 360, 504, 660だけである．位数が60の単純群は $\mathfrak{A}_5$ だけであり，位数が360の単純群は $\mathfrak{A}_6$ だけである．位数168および660のものは $L(2, 7)$ および $L(2, 11)$ である．したがって，$L(2, 5)\cong\mathfrak{A}_5$ であるが，さらに，K を4つの元からなる体とすると，$L(2, K)\cong L(2, 5)$ であることがわかっている．また，$L(3, 2)$ の位数は168であるが，実際は $L(3, 2)\cong L(2, 7)$ である．

問 題 5

1. 群 G の位数 p^m の部分群 H が p-シロー群 P に含まれるための必要十分条件は，$H\subset N(P)$ が成り立つことである．

2. 位数が $p^m q^n$（p, q は異なる素数）の群 G の p-シロー群を P, q-シロー群を Q とすれば $G=PQ$.

3. P を群 G の p-シロー群，N を G の正規部分群，$N(P)$ を P の正規化群とすると，

(1) N の p-シロー群 $P^*=P\cap N$ の G における正規化群を $N(P^*)$ とすると，$N(P)\subset N(P^*)$.

(2) $N(P)N/N$ は G/N の p-シロー群 PN/N の正規化群である．

(3) $N(P^*)N=G$, したがって

1) 巻末文献〔10〕参照．

$$N(P^*)/N(P^*) \cap N \cong G/N.$$

4. H は群 G の部分群で，$|G: H|$ が素数 p の巾とする．P を G の p-シロー群とすれば，$G=HP=PH$ で，$H\cap P$ は H の p-シロー群である．

5. P は群 G の p-シロー群で，K, L は P の部分集合とする．K, L のそれぞれの正規化群が P を含み，しかも K と L が G で共役ならば，K と L は $N(P)$ で共役である．したがって，K, L が P の正規部分群で，G で共役ならば，K, L は $N(P)$ で共役である．

6. 位数が 15, 35 および 119 の群はすべて巡回群である．

7. 非可換な群 G の位数 g が，つぎの場合，そのシロー群の個数を求めよ．

(1) $g=21$　(2) $g=39$　(3) $g=253$

8. 位数が 255 の群 G は巡回群である．

9. 位数が 12, 30 の群は可解群である．

10. 位数が p^2q （p, q は異なる素数）の群は可解群である．

11. 位数が 24 の群は可解群である．

12. 位数が $2p$ （p は奇素数）の群を決定せよ．

13. 位数 p^n の群の位数 p^{n-1} の部分群は正規部分群である．

14. G は非可換な p-群で，その位数が p^3 ならば，$Z(G)=D(G)$, $|Z(G)|=p$ であり，$G/Z(G)$ は不変系が (p, p) のアーベル群である．

15. 位数が $2^3\cdot 7\cdot 11$ の群は単純群ではない．

16. 位数が p^2q^2 （p, q は異なる素数）の群は単純群ではない．

17. G は位数が mp （p は素数で，$m\neq 1$, $p\nmid m$ とする）の単純群とする．P を G の p-シロー群とすれば $|N(P) : Z(P)|$ は $p-1$ の約数である．

問 題 解 答

1 章

p. 2　問 1.　1) 閉じている　2) 閉じていない

問 2.　1) 閉じている　2) 閉じていない　3) 閉じている

p. 3　問 3.　みたしている

問 4.　1) 可換である　2) 可換でない

問 5.　1), 2), 3) すべてみたす

問 6.　1) みたさない　2) みたさない

p. 5　問 1.　$x>0$ なら 2 つ, $x=0$ のとき 1 つ

問 2.　1 つ

p. 8　問 2.　fg は AD, BC の中点を結ぶ直線に関する鏡映

p. 10　問 1.　1) G－4　2) G－4

p. 28　問 3.　$(\alpha_1\ \alpha_2 \cdots\cdots \alpha_r)=(\alpha_1\ \alpha_r)\cdots\cdots(\alpha_1\ \alpha_2)$ であることから出る.

p. 30　問 1.　$\varphi(n)=2n$ とおいてみよ.

p. 31　**問題 1**

1.　(1, 0) が単位元となる.

3.　$|a\circ b|<1$ を示すため, $1-a\circ b>0$, $1+a\circ b>0$ を示せ. 単位元は 0, a の逆元は $-a$.

5.　$\sigma=(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ で生成された巡回群 H の元は $e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5=\sigma^{-3}, \sigma^6=\sigma^{-2}, \sigma^7=\sigma^{-1}$ である. $\sigma^2=(1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$

$\sigma^3=(1\ 4\ 7\ 2\ 5\ 8\ 3\ 6)$

$\sigma^4=(1\ 5)(2\ 6)(3\ 7)(4\ 8)$

$\sigma^5=\sigma^{-3}=(6\ 3\ 8\ 5\ 2\ 7\ 4\ 1)$

$\sigma^6=\sigma^{-2}=(7\ 5\ 3\ 1)(8\ 6\ 4\ 2)$

$\sigma^7=\sigma^{-1}=(8\ 7\ 6\ 5\ 4\ 3\ 2\ 1)$

6.　$(2\ 3\ 4)(1\ 2)(2\ 3\ 4)^{-1}=(1\ 3)$,　$(2\ 3\ 4)(1\ 3)(2\ 3\ 4)=(1\ 4)$ であるから, $(1\ 2), (1\ 3), (1\ 4)\in\mathfrak{S}_4$ である.

7.　正 6 角形に垂直な軸のまわりの回転に対しては, e, $(1\ 2\ 3\ 4\ 5\ 6)$,

(1 3 5)(2 4 6), (1 4)(2 5)(3 6), (1 5 3)(2 6 4), (6 5 4 3 2 1). 向かい合う頂点を結ぶ直線に関する鏡映には (2 6)(3 5), (1 3)(4 6), (1 5)(2 4). 向かい合う2辺の中点を結ぶ直線に関する鏡映には (1 2)(3 6)(4 5), (1 6)(2 5)(3 4), (1 4)(2 3)(5 6).

9. 1) v の位数は 4, u の位数は 2. $vu=uv^3$

2) y の位数は n, x の位数は 2. $yx=xy^{n-1}$

2 章

p. 36 問 1. $(ba)^{s-1}=a^{-1}b^{-1}=(ba)^{-1}$ $\therefore$ $(ba)^s=e$. $o(ba)=t$ とおくと $t|s$. 同様にして $s|t$ $\therefore$ $t=s$

p. 37 問 3. $G\ni a\neq 0$ のつくる巡回群 $\langle a\rangle=G$. a の位数 n が合成数で $n=kl$, $k, l>1$, ならば, $\langle a^k\rangle$ は G の真の部分群である.

p. 46 問 3. $HN<G$ であるから,

$|G:H|=|G:HN||HN:H|=|G:HN||N:H\cap N|$

p. 46 問 4. $|G:H\cap K|=|G:H||H:H\cap K|$ であるから, $|G:K|$ は $|H:H\cap K|=HK$ に含まれる K を法とした右剰余類の個数 m の約数ゆえ, m に等しい. $\therefore$ $G=HK$.

p. 56 問 3. 群 G の中心 $Z\ni a \Leftrightarrow a$ は1つだけで共役類をつくることに注意せよ. または関係 $\sigma\tau=\tau\sigma^3$ を使ってもよい.

p. 62 **問題 2**

4. $H\ni h$, $K\ni k$ のとき $hkh^{-1}k^{-1}=hkh^{-1}\cdot k^{-1}=h\cdot kh^{-1}k^{-1}$ は, H にも K にも入るから, 単位元.

5. 左剰余類 Ha は HaH に含まれるから, $HaH=Ha$.

$\therefore$ $aH=H^{-1}Ha=Ha$, $\therefore$ $a\in N(H)$

7. H を $\boldsymbol{R}^*$ の指数有限 $n>1$ の部分群とする. n が奇数ならば, 任意の実数 $\alpha\neq 0$ に対し $\sqrt[n]{\alpha}$ は存在し, $\alpha=(\sqrt[n]{\alpha})^n\in H$ であるから $\boldsymbol{R}^*=H$ となってしまう. したがって, n は偶数. そうすると任意の $\alpha>0$ に対して $\sqrt[n]{\alpha}$ が存在するから, $\alpha=(\sqrt[n]{\alpha})^n\in H$ で, $P\subset H$ となる. つぎに, H を加法群 $\boldsymbol{R}$ の指数有限 $m>1$ の部分群とすれば, 任意の実数 α に対して, $\alpha/m\in$

$\boldsymbol{R}$, $m(\alpha/m)=\alpha\in H$ ゆえ，$H=\boldsymbol{R}$ となってしまう．$\boldsymbol{P}\ni\alpha\longmapsto\log\alpha\in\boldsymbol{R}$ により $P\cong\boldsymbol{R}$.

9.　中心元はとくに$\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$と可換である．

また，$\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}1&\tau\\0&1\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}^{-1}=\begin{pmatrix}1&0\\-\tau&1\end{pmatrix}$である．

10.　$n=2m$ に対し，m 次2面体群 D_m をとればよい．

11.　(1) まず $ba=a^3b$. したがって，$ba^2=a^2b$, $ba^3=ab$. さらに $(a^ib)a^j=a^{i-j}b$, $(a^ib)(a^jb)=a^{i-j+2}$, とくに $(a^ib)(a^{i-2}b)=e$. Q の中で，巡回群 $\langle a\rangle$ と剰余類 $\langle a\rangle b$ の和集合は群をつくる．この群は a, b を含むから，Q 全体になる．$\langle a\rangle$ の位数は4であるから，$|Q|=8$. Q は非可換群である．$Q=\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

(2) Q の部分群の位数は4か2である．位数4の部分群は指数が2であるから，正規部分群である．位数2の部分群は $\langle a^2\rangle$ だけである．$(a^jb)a^2(a^jb)^{-1}=a^jba^2b^{-1}a^{-j}=a^ja^2a^{-j}=a^2$ より $\langle a^2\rangle\lhd G$.

(3) $a\longmapsto i$, $b\longmapsto j$ とせよ．$ab\longmapsto ij=k$ となる．(4元数群の任意の元 u の共役は u か $-u$ である．したがって部分群 $H\ni u$ ならば，$-1=u^2\in H$, $-u=u^3=u^{-1}\in H$. ∴ $H\lhd G$)

12.　A の位数は4で，$A^2=-E=B^2$, $BAB^{-1}=A^{-1}$

13.　$a\longmapsto i$, $b\longmapsto j$, $c\longmapsto k$ によって，4元数群と同型になる．

14.　$ba^ib^{-1}=a^{-i}$, $(a^ib)a^j=a^{i-j}b$, $(a^ib)(a^jb)=a^{i-j}b^2=a^{i-j+2^{n-2}}$. したがって，$a, b$ で生成された群 Q_n の中で巡回群 $\langle a\rangle$ と剰余類 $\langle a\rangle b$ の和集合は部分群 H をつくる．$a, b\in H$ であるから，$H=Q_n$. $\langle a\rangle$ の位数が 2^{n-1}, ∴ $|Q_n|=2^n$.

15.　$H=\langle xy\rangle$ とおく．$x^2=y^2=e$ より，$x^{-1}xyx=y^{-1}x^{-1}=(xy)^{-1}$, $y^{-1}xyy=y^{-1}x^{-1}=(xy)^{-1}$ で，$x^{-1}Hx=y^{-1}Hy=H$. G の任意元 u に対し $u^{-1}Hu=H$, $H\lhd G=\langle x, y\rangle$. $yx=y^{-1}x^{-1}=(xy)^{-1}\in H$ で，$y=yxx\in Hx$ であるから，$G=H\cup Hx$. G は巡回群でないから $H\neq G$. ∴ $|G:H|=2$. もしも $|G|=2n$ ならば，H の，したがって，xy の位数は n であるから，$xy\longmapsto\sigma$, $x\longmapsto\tau$ とすれば，G は D_n と同型になる．実際 $(xy)^{n-1}=(xy)^{-1}=y^{-1}x^{-1}=yx$ であるから，$(xy)x=x(yx)=x(xy)^{n-1}$.

16.　$|HN:N|=|H:H\cap N|$ は $|H|$ の約数であり，$|G:N|$ の約数であるか

ら，1に等しい．∴ $HN=N$. ∴ $H\subset N$.

17. Hが位数m', $m'|m$, の部分群ならば，m'とrは互いに素であるから，問題16 より$H\subset N$.

18. $|N:H\cap N|=|HN:H|$ は $|G:H|$ の約数であり，$|N|$ の約数であるから，1に等しい．∴ $N=H\cap N$. ∴ $N\subset H$.

19. $K\supset K\cap H_2$ より $H_1K\supset H_1(K\cap H_2)$. $H_2\supset H_1$, $H_2\supset K\cap H_2$ より $H_2\supset H_1(K\cap H_2)$. ∴ $H_1K\cap H_2\supset H_1(K\cap H_2)$. 逆に $H_1K\cap H_2\ni a$ として $a=bc$, $b\in H_1$, $c\in K$, とすれば，$c=b^{-1}a\in H_1H_2=H_2$.
∴ $c\in K\cap H_2$, $a=bc\in H_1(K\cap H_2)$. ∴ $H_1K\cap H_2=H_1(K\cap H_2)$.

20. $H_1=H_1(H_1\cap K)=H_1(H_2\cap K)$. $H_1(H_2\cap K)\subset H_1H_2\cap H_1K=H_2\cap H_1K$. 逆に $H_1K\cap H_2\ni a=bc$, $b\in H_1$, $c\in K$ とすれば，$c=b^{-1}a\in H_1H_2=H_2$ であるから，$c\in K\cap H_2$, $a=bc\in H_1(K\cap H_2)$.

$$\therefore\ H_1=H_1(H_2\cap K)=H_1K\cap H_2=H_2K\cap H_2=H_2.$$

21. $|K_2:K_1|=|K_2:H_1||H_1:H_1\cap H_2|=|K_2:H_1|\times$($H_1H_2$ に含まれる法 H_2 の右剰余類の個数)$\leqq|K_2:H_1|\times|K_2:H_2|$($\because$ $K_2=\langle H_1, H_2\rangle\supset H_1H_2$). すなわち，$|K_2|/|K_1|\leqq(|K_2|/|H_2|)\times(|K_2|/|H_1|)$. したがって $|H_1||H_2|\leqq|K_1||K_2|$. ここで，等号が成り立つ $\Leftrightarrow$ H_1H_2 に含まれる法 H_2 の剰余類の個数$=|K_2:H_2|$ $\Leftrightarrow$ $K_2=H_1H_2$ (p. 46，定理 10).

22. $|G|=n$, $|G:H|=h$ とする．$H\subset N(H)$ であるから，Hの共役群の個数はたかだかhで，これらは少なくとも単位元eを共有するから，共役群全体の和集合の元は多くとも $1+(|H|-1)h=1+n-h<n$.

23. $H\subset N(H)$ であるから，Hの共役群の個数は $|G:H|$ を越さないから，有限m. 共役を $H_1, H_2, \cdots\cdots, H_m$ とすれば，$\bigcap H_i$, iは1からmまで動く，はGの正規部分群で，その指数は有限である．(p, 46，定理10系).

24. 問題23よりHはGの指数有限な正規部分群Nを含む．H/Nは有限群 G/N の部分群であるから，問題22より，H/Nのどの共役群 yHy^{-1}/Nにも含まれない右剰余類xNが存在する．

このとき $x\notin yHy^{-1}$ $\forall y\in G$.

25. 問題23よりHはGの指数有限な正規部分群Nを含む．
H/NはG/Nの指数nの部分群である．いま，かりに $G/N=(H/N)\bar{c}_1+\cdots\cdots+(H/N)\bar{c}_n=\bar{c}_1(H/N)+\cdots\cdots+\bar{c}_n(H/N)$ だとする．G/Nの元

$\bar{c}_1, \bar{c}_2, \cdots\cdots, \bar{c}_n$ の任意の代表元を $a_1, a_2, \cdots\cdots, a_n$ とするとき，$\bar{c}_i=a_iN=Na_i$. G の任意の元 x の法 N の剰余類 $\bar{x}=xN\in(H/N)\bar{c}_i=(H/N)Na_i=\{hNNa_i=hNa_i, h\in H\}$ ならば，$x\in hNa_i\subset Ha_i$. 同様にして，$x\in a_jH$. $\therefore G=\bigcup Ha_i=\bigcup a_iH$. いま，$i\neq k$ で，$Ha_i\cap Ha_k\ni x$ とすると，$x=ha_i=h'a_k$ であるから，$h^{-1}h'=a_ia_k^{-1}\in H$, $\therefore Na_i\equiv Na_k \pmod{H/N}_l$. したがって，$\bar{c}_i=\bar{c}_k$ となってしまうから，$Ha_i\cap Ha_k=\phi$. ゆえに，$a_1, a_2, \cdots\cdots, a_n$ は G の法 H の左完全代表系である．同様にして，$a_1, a_2, \cdots\cdots, a_n$ は G の法 H の右完全代表系であることがいえる．そこで，有限群である G/N について，証明すればよい．すなわち，G は有限群だと仮定してよい．G を H を法として両側分解し，$G=Hb_1H+\cdots\cdots+Hb_rH$, $(b_1=e)$ とすれば，$Hb_iH=Hb_ig_{i1}+\cdots\cdots+Hb_ig_{in(i)}$, $g_{ij}\in H$, $n(i)=|H:H\cap b_i^{-1}Hb_i|$, $Hb_iH=h_{i1}b_iH+\cdots\cdots+h_{im(i)}b_ih$, $h_{ij}\in H$, $m(i)=|H:H\cap b_iHb_i^{-1}|$ (p. 45, 定理 9). $b_i(H\cap b_i^{-1}Hb_i)b_i^{-1}=b_iHb_i^{-1}\cap H$ であるから，$n(i)=m(i)$. そこで $b_{ij}=h_{ij}b_ig_{ij}$ とすれば，$Hb_iH=Hb_{i1}+\cdots\cdots+Hb_{in(i)}=b_{i1}H+\cdots\cdots+b_{in(i)}H$. そこで b_{ij}, $1\leqq i\leqq r$, $1\leqq j\leqq n(i)$, を $a_1, a_2, \cdots\cdots, a_n$ とすればよい．

3 章

p. 68　問 1．$G=\langle a\rangle$；$G'=\langle a'\rangle$ のとき，$a\longmapsto a'$ とすればよい．G' が無限巡回群なら，核は $\{e\}$, G' が位数 n の有限巡回群ならば，核は $\langle a^n\rangle$.

p. 71　問 1．位数 3 の巡回群 $\langle a\rangle$ の自己同型は $I: a\longmapsto a$ と，$\sigma: a\longmapsto a^2$ だけで，$\sigma^2=I$. 位数 4 の巡回群 $\langle a\rangle$ の自己同型は $I: a\longmapsto a$ と $\tau: a\longmapsto a^3$ だけで，$\tau^2=I$.

問 3．$G=\langle a\rangle$ を位数 p^n-1 の巡回群とすれば，G において，$\sigma: a\longmapsto a^p$ は G の自己同型で，σ の位数は n である．一方，$A(G)$ の位数は $\varphi(p^n-1)$ である．

p. 72　問 4．$\mathfrak{S}_3$ の中心は e のみであるから，$I(\mathfrak{S}_3)\cong\mathfrak{S}_3$ であり，$\mathfrak{S}_3$ は 6 個の内部自己同型をもつ．一方，$\mathfrak{S}_3$ の自己同型は位数 2 の元を同じく位数 2 の元にうつすので，(1 2), (1 3), (2 3) の間の置換を引き起こす．自己同型 σ, τ の引き起こす置換が同じとき，$\mathfrak{S}_3$ は(1 2), (1 3), (2 3) で生成されているから，$\sigma=\tau$ となる．したがって，$\mathfrak{S}_3$ はたかだか $3!=6$ 個の自己同

型しかもたない．ゆえに，$\mathfrak{S}_3$ の自己同型はすべて内部自己同型で，$A(\mathfrak{S}_3)=I(\mathfrak{S}_3)\cong\mathfrak{S}_3$.

問 6．$\mathfrak{A}_4$ は位数 3 の元を 8 個，位数 2 の元を 3 個含む．$\mathfrak{A}_4=\langle(1\ 2\ 3),(1\ 2)(3\ 4)\rangle$ である．$\mathfrak{A}_4$ の自己同型は $(1\ 2\ 3)$ と $(1\ 2)(3\ 4)$ の行先で決まるから，自己同型はたかだか $8\times3=24$ 個．一方，$\mathfrak{S}_4$ の元 σ によって引き起こされる内部自己同型 $T_\sigma:\tau\longmapsto\sigma\tau\sigma^{-1}$ は $\mathfrak{A}_4$ の自己同型 T_σ^* を引き起こし，$T_\sigma\neq T_{\sigma'}$ ならば，$T_\sigma^*\neq T_{\sigma'}^*$．したがって，$I(\mathfrak{S}_4)\cong\mathfrak{S}_4$ であるから，$\mathfrak{A}_4$ は 24 個の自己同型をもち，それは，すべて $\mathfrak{S}_4$ の内部自己同型で引き起こされるから，$A(\mathfrak{A}_4)=I(\mathfrak{S}_4)\cong\mathfrak{S}_4$.

問 7．$\mathfrak{A}_4$ の中心 $Z=\{e\}$（p. 60 の $\mathfrak{A}_4$ 共役類）である．

p. 73　**問題 3**

1. 第 2 章の問題 7 より $\boldsymbol{R}^*$ は指数が 2 の部分群 $P=\{\alpha>0\}$ を含むが，$\boldsymbol{R}$ は指数有限の部分群を含まない．

2. $a_i'H'\cap a_j'H'\ni x$ とすると $a_i'h_1'=a_j'h_2'$, $h_1, h_2\in H'$. $\therefore\ \varphi(a_i^{-1}a_j)=a_i'^{-1}a_j'=h_1'h_2'^{-1}\in H'$. したがって，$a_i^{-1}a_j\in H$. $\therefore\ i=j$. そこで $i\neq j$ ならば，$a_i'H'\cap a_j'H'=\phi$. G' の任意元 $x'=\varphi(x)$, $x=a_ih\in G$ ゆえ，$x'\in a_i'H'$.

3. $G_1\triangleright G_2$, $G_1>G_1\cap H$ であるから，$(G_1\cap H)G_2$ は G_1 の部分群である．$(G_1\cap H)G_2/G_2\cong(G_1\cap H)/G_1\cap H\cap G_2=(G_1\cap H)/(G_2\cap H)$.

8. $V=\{e, a, b, c\}$ の自己同型は，a, b, c の置換を引き起こす．逆に，a, b, c の任意の置換によって，V の自己同型が決まる．

4 章

p. 95　問 2．$H, K\supset D(G)$ ゆえ $H\cap K\supset D(G)$ であるから．

p. 96　問 3．$\mathfrak{A}_4/V$ は位数 3 の巡回群であるから，$V\supset D(\mathfrak{A}_4)$．しかし，$V$ の真の部分群，たとえば，$\langle(1\ 2)(3\ 4)\rangle$ は $\mathfrak{A}_4$ の正規部分群でない．
$(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1}=(2\ 3)(1\ 4)$ であるからである．$D(\mathfrak{A}_4)$ は $\mathfrak{A}_4$ の正規部分群であるから，$D(\mathfrak{A}_4)$は V の位数 2 の部分群ではない．
$\mathfrak{A}_4$は非可換群であるから，$D(\mathfrak{A}_4)$ は単位群でもない．$\therefore\ D(\mathfrak{A}_4)=V$.

p. 97　問 4．G/N の可換正規鎖を $G/N=G_0/N\supset G_1/N\supset\cdots\cdots\supset G_r/N=N/N$，$N$ の可換正規鎖を $N=N_0\supset N_1\supset\cdots\cdots\supset N_s=\{e\}$ とすれば，$G=G_0\supset G_1\supset\cdots\cdots\supset N=N_0\supset\cdots\cdots\supset N_s=\{e\}$ は G の可換正規鎖である．

$(G_i/N)/(G_{i+1}/N)\cong G_i/G_{i+1}$ に注意せよ．

p. 98 問 5．N を $\mathfrak{S}_n$ の真の部分群とする．$\mathfrak{A}_n$ は単純群であるから $\mathfrak{A}_n$ の正規部分群 $\mathfrak{A}_n\cap N=\mathfrak{A}_n$ か $=\{e\}$．$\mathfrak{A}_n\cap N=\mathfrak{A}_n$ ならば，$N=\mathfrak{A}_n$．$\mathfrak{A}_n\cap N=\{e\}$ とすれば，$\mathfrak{A}_n\otimes N=\mathfrak{S}_n$ であり，N の位数は 2 となる．しかし，$\mathfrak{S}_n$ は位数 2 の正規部分群を含まない．位数 2 の置換を共通の文字を含まない巡回置換の積に分解すると，その巡回置換はすべて互換であるから，$\sigma=(\alpha_1\ \beta_1)(\alpha_2\ \beta_2)\cdots\cdots(\alpha_r\ \beta_r)$ で，$(\alpha_1\ \alpha_2)\sigma(\alpha_1\ \alpha_2)^{-1}=(\alpha_2\ \beta_1)(\alpha_1\ \beta_2)\cdots\cdots(\alpha_r\ \beta_r)\neq\sigma$ であるからである．$\sigma=(\alpha\ \beta)$ なら $\tau=(\beta\ \gamma)$ として，$\tau\sigma\tau^{-1}=(\alpha\ \gamma)\neq\sigma$ となる．

問 6．$\mathfrak{S}_5$ が可解群とすれば，$\mathfrak{A}_5$ も可解群である．$\mathfrak{A}_5$ は非可換であるから，$\mathfrak{A}_5$ は真の正規部分群を含まなくてはならないが，$\mathfrak{A}_5$ の共役類の分類から，そのような部分群は存在しない．(p. 61，例題 4)．したがって，$\mathfrak{S}_5$ は可解でない．$\mathfrak{S}_n(n\geqq 6)$ は $\mathfrak{S}_5$ と同型な部分群を含むから可解でない．

p.98 **問題 4**

1. $H\otimes K\ni hk\longmapsto h\in H$ は $H\otimes K$ から H の上への準同型で，その核は K である．

2. $Z(H)\otimes Z(K)\subset Z(G)$ は明らか．$Z(G)\ni hk$, $h\in H$, $k\in K$ とする．H の任意元 a に対して，$(hk)a=(ha)k$, $a(hk)=(ah)k$ であるから，$ha=ah$ $\therefore$ $h\in Z(H)$．同じく $k\in Z(K)$．$\therefore$ $hk\in Z(H)\otimes Z(K)$, $Z(G)=Z(H)\otimes Z(K)$.

4. f_i を G から G/N_i の上への自然な準同型とし，G から $G/N_1\otimes\cdots\cdots\otimes G/N_r$ への準同型 f を $f(a)=(f_1(a),\cdots\cdots,f_r(a))$ とする．$f(a)=1\Leftrightarrow f_i(a)=1\quad\forall i\Leftrightarrow a\in N_i\quad\forall i\Leftrightarrow a=e$
$G\cong f(G)\subset G/N_1\otimes\cdots\cdots\otimes G/N_r$

5. 問題 4 より G は $G/H\otimes G/K$ の部分群に同型である．

6. $G/M\cap N$ の中で，$(M/M\cap N)\cap(N/M\cap N)=1$ で，$M/M\cap N$, $N/M\cap N\lhd G/M\cap N$ であるから，$G/M\cap N=MN/M\cap N=M/M\cap N\otimes N/M\cap N$．また，$G/N=MN/N\cong M/M\cap N$, $G/M\cong MN/M\cong N/M\cap N$ $\therefore$ $G/M\cap N\cong G/N\otimes G/M$.

7. $\overline{H}_1\ni a_1,\ a_1'$ とすると，$a_1a_2=b\in H$, $a_2\in G_2$, $a_1'a_2'=b'\in H$, $a_2'\in G_2$. $bb'^{-1}=a_1a_2(a_1'a_2')^{-1}=a_1a_1'^{-1}\cdot a_2a_2'^{-1}$ で，bb'^{-1} の G_1 成分は $a_1a_1'^{-1}$ であるから，$a_1a_1'^{-1}\in\overline{H}_1$．したがって $\overline{H}_1<G_1$．同様にして，$\overline{H}_2<G_2$．$H_i\subset\overline{H}_i$ は明ら

か. $H\ni b=a_1a_2$ に対し $a_1H_1a_1^{-1}\subset G_1$, $a_1H_1a_1^{-1}=a_1a_2H_1a_2^{-1}a_1^{-1}=bH_1b^{-1}\subset H$ ゆえ, $a_1H_1a_1^{-1}\subset H\cap G_1=H_1$ となり, $H_1\lhd\bar{H}_1$. 同様に, $H_2\lhd\bar{H}_2$. つぎに H の元 b と b' の G_1 成分が一致するとして, $b=a_1a_2$, $b'=a_1a_2'$ とすれば, $bb'^{-1}=a_2a_2'^{-1}\in H\cap G_2=H_2$ ゆえ, $H_2a_2=H_2a_2'$. したがって, $\bar{H}_1$の元 a_1 に対して, $a_1a_2\in H$ ならば, H_2a_2 は一意的に決まる. $\varphi: a_1\longmapsto H_2a_2$ とする. いま, $\bar{H}_1\ni a_1'$, $a_1'a_2'\in H$ のとき $\varphi: a_1'\longmapsto H_2a_2'$ であり, $a_1a_2a_1'a_2'=a_1a_1'a_2a_2'\in H$ であるから, $\varphi(a_1a_1')=H_2a_2a_2'=H_2a_2H_2a_2'=\varphi(a_1)\varphi(a_1')$ となり, φ は $\bar{H}_1$ から $\bar{H}_2/H_2$ の上への準同型. ここで, φ の核$=\{a_1\in\bar{H}_1,\ a_1\in H\}=H_1$ である. したがって, $\bar{H}_1/H_1\cong\bar{H}_2/H_2$.

8. 問題7を使うと $\bar{H}_1/H_1\cong\bar{H}_2/H_2$. $|\bar{H}_1|$ と $|\bar{H}_2|$ は互いに素であり, $|\bar{H}_1/H_1|$, $|\bar{H}_2/H_2|$ も互いに素であるから, $\bar{H}_1/H_1=1$, $\bar{H}_2/H_2=1$, $\bar{H}_1=H_1$, $\bar{H}_2=H_2$. H_1, H_2 の位数は互いに素であるから, $H_1\cap H_2=\{e\}$. H の元は $\bar{H}_1=H_1$ の元と $\bar{H}_2=H_2$ の元の積に表せるから $H=H_1\otimes H_2$.

9. $A(G_1)\ni\sigma_1$, $A(G_2)\ni\sigma_2$ のとき,
$[\sigma_1, \sigma_2]: (x_1, x_2)\longmapsto(\sigma_1(x_1), \sigma_2(x_2))$ は $G_1\otimes G_2$ の自己同型で, $(\sigma_1, \sigma_2)\longmapsto[\sigma_1, \sigma_2]$ は $A(G_1)\otimes A(G_2)$ から $A(G_1\otimes G_2)$ への同型である. 上への写像であることをいう. $A(G_1\otimes G_2)\ni\rho$ とする. $\rho(x_1, e)\in G_1\otimes G_2$ ゆえ, $\rho(x_1, e)=(\sigma(x_1), \rho'(x_1))$ と書ける. このとき, σ は G_1 から G_1 への準同型, ρ' は G_1 から G_2 への準同型である. ところで, $|G_1|$, $|G_2|$ が互いに素であるから, $\rho'(x_1)=e$, $\forall x_1\in G_1$. $\therefore\ \rho(x_1, e)=(\sigma(x_1), e)$. ρ が1対1であるから σ も1対1で, G_1 が有限群であるから, σ は G_1 の自己同型になり, $\sigma\in A(G_1)$. 同様にして, $\rho(e, x_2)=(e, \tau(x_2))$ で, $\tau\in A(G_2)$. したがって, $\rho(x_1, x_2)=\rho((x_1, e)(e, x_2))=\rho(x_1, e)\rho(e, x_2)=(\sigma(x_1), e)(e, \tau(x_2))=(\sigma(x_1), \tau(x_2))$ となり, $\rho=[\sigma, \tau]$.

10. $G=\langle a_5\rangle\otimes\langle a_3\rangle\otimes\langle a_2\rangle\otimes\langle b_1\rangle\otimes\langle b_2\rangle$ で, $\langle a_i\rangle$ の位数を p^i, $\langle b_1\rangle$, $\langle b_2\rangle$ の位数を p とすれば, $G^{(p)}=\langle a_5{}^p\rangle\otimes\langle a_3{}^p\rangle\otimes\langle a_2{}^p\rangle$ で, $\langle a_i{}^p\rangle$ の位数は p^{i-1} である.

11. $G=\langle a_1\rangle\otimes\cdots\cdots\otimes\langle a_s\rangle$, 各 a_i の位数は q_i と直積分解する. $u_i=q_i/q_i'$, $a_i{}^{u_i}=b_i$ とおくと, $H=\langle b_1\rangle\otimes\cdots\cdots\otimes\langle b_t\rangle$ の不変系は $(q_1', \cdots\cdots, q_t')$. また, $\langle a_1{}^{q_1'}\rangle\otimes\cdots\cdots\otimes\langle a_t{}^{q_t'}\rangle\otimes\langle a_{t+1}\rangle\otimes\cdots\cdots\otimes\langle a_s\rangle=N$ とすると, G/Nの不変系は, 上記 H の不変系と同じになる.

12. G を巡回群の直積に分解してみよ.

13. 位数 p^2 の部分群 H はやはり基本アーベル群である.

$H=\langle a_1\rangle\otimes\langle a_2\rangle$ として, H に含まれない元 a_3 をとれば, H と $\langle a_3\rangle$の積は直積 $H\otimes\langle a_3\rangle$ である. この直積に含まれない元 a_4 をとると, $H\otimes\langle a_3\rangle$ と $\langle a_4\rangle$ の積は直積で, G に等しい. 逆に $G=\langle b_1\rangle\otimes\langle b_2\rangle\otimes\langle b_3\rangle\otimes\langle b_4\rangle$ とすれば, $\langle b_1\rangle\otimes\langle b_2\rangle$ は位数 p^2 の部分群である. 位数 p^2 の部分群を生成する 2つの元の対 a_1, a_2 の個数は全部で $(p^4-1)(p^4-p)$ あり, 位数 p^2 の1つの部分群を生成する対は $(p^2-1)(p^2-p)$ ずつあるから, 位数 p^2 の部分群の個数$=(p^4-1)(p^4-p)/(p^2-1)(p^2-p)=(p^4-1)(p^3-1)/(p^2-1)(p-1)$.
同様にして, 位数 p^3 の 部分群の個数$=(p^4-1)(p^4-p)(p^4-p^2)\div$
$(p^3-1)(p^3-p)(p^3-p^2)=(p^4-1)/(p-1)$.

問題16に示した指標に関する双対定理を使えば, 位数 p^3 の部分群は, 指数 p の部分群で, それに1対1に G の指標群 $X(G)$ の位数 p の部分群が対応している. $X(G)\cong G$ であるから, $X(G)$ における位数 p の部分群の個数は, G におけるそれと等しい. G の位数 p の部分群は, G の単位元以外の任意の元で生成される. $\langle a\rangle$ と同じ群を生成するものは a^i, $i=1, 2, \cdots\cdots, p-1$, の $p-1$ 個あるから, 位数 p の部分群の個数は
$(p^4-1)/(p-1)$.

14. $p_1, p_2, \cdots\cdots, p_r$ を G の位数の素因数とする. 位数が p_i の巾で最大な元を a_i, その位数を $p_i^{\lambda_i}$ とする. $a=a_1a_2\cdots\cdots a_r$ の 位数は $p_1^{\lambda_1}p_2^{\lambda_2}\cdots\cdots p_r^{\lambda_r}$. G の任意元 x の位数 $n=p_1^{\mu_1}p_2^{\mu_2}\cdots\cdots p_r^{\mu_r}$ で, 巡回群 $\langle x\rangle$ は位数 $p_i^{\mu_i}$ の巡回群 H_i の直積となるから, $x=x_1x_2\cdots\cdots x_r$, 各 x_i の位数 $p_i^{\mu_i}\leqq p_i^{\lambda_i}$.
$\therefore$ $n\leqq p_1^{\lambda_1}p_2^{\lambda_2}\cdots\cdots p_r^{\lambda_r}$. したがって $m=p_1^{\lambda_1}p^{\lambda_2}\cdots\cdots p_r^{\lambda_r}$ であり, $n|m$ であるから, $x^m=e$.

15. $n=p_1^{e_1}\cdots\cdots p_r^{e_r}$ を素因数分解とすれば, $G=P_1\otimes\cdots\cdots\otimes P_r$, 各 P_i は位数 $p_i^{e_i}$ のアーベル群となる. $m|n$ ならば, $m=p_1^{f_1}\cdots\cdots p_r^{f_r}$ で, $f_i\leqq e_i$.
そこで, 位数が素数巾 p^e のアーベル群に対して, 証明すればよい. e に関する帰納法を使え.

16. (1) $G_H{}^*$ が G^* の部分群であることはすぐわかる. $G_H{}^*\ni\chi$ は $\chi(xh)=\chi(x)$ $\forall h\in H$ であるから, $\bar{\chi}(xH)=\chi(x)$ によって, χ は G/H の指標 $\bar{\chi}$ を引き起こす. $G_H{}^*\ni\chi_1, \chi_2$ が $\chi_1\neq\chi_2$ であれば, $\bar{\chi}_1\neq\bar{\chi}_2$ である. 逆に G/H の指標 $\bar{\chi}$ に対して, $\chi(x)=\bar{\chi}(xH)$ とおけば, χ は G の指標で, $\chi\in G_H{}^*$ である. このようにして, $G_H{}^*\ni\chi$ は G/H の指標と考えられ, $G_H{}^*$

は G/H の指標群となるから，$G_H{}^* = X(G/H) \cong G/H$.

(2) $G_H{}^*$ が G の部分群であることはすぐわかる．p. 92，定理11のあとで示したように，G は $X^2(G) = X(G^*) = G^{**}$ と $a \longmapsto \hat{a}$ によって同型であり，$G_H{}^*$ には $G_H{}^{***} = \{\hat{a} | \hat{a} \in G^{**},\ \hat{a}(\chi) = 1 \quad \forall \chi \in H^*\}$ が対応する．(1)によって $G_H{}^{***} = X(G^*/H^*) \cong G^*/H^*$ であるから，$G_H{}^* \cong G^*/H^*$.

17. $G/N = HN/N \cong H/H \cap N$ で，H が可解であるから，$H/H \cap N$ は可解，したがって G/N は可解．N が可解であるから，G 自身可解である．

18. $(\alpha\ \beta\ \gamma) = (\alpha\ \beta\ \delta)(\alpha\ \beta\ \varepsilon)(\alpha\ \beta\ \delta)^{-1}(\alpha\ \beta\ \varepsilon)^{-1}$ である．かりに，$\mathfrak{S}_n$ を可解として，$\mathfrak{S}_n$ の可換正規鎖を $\mathfrak{S}_n = G_0 \supsetneqq G_1 \supset \cdots\cdots \supset G_r = \{e\}$ とすると，G_0/G_1 がアーベル群であるから，$G_1 \supset D(\mathfrak{S}_n) = \mathfrak{A}_n$ となり，$G_1 = \mathfrak{A}_n$．$G_1 \supset G_2 \cdots\cdots \supset G_r = \{e\}$ は $\mathfrak{A}_n$ の可換正規鎖となる．しかし，$D(\mathfrak{A}_n) = \mathfrak{A}_n$ で，$\mathfrak{A}_n$ は非可換であるから，可換正規鎖をもたない．これは矛盾である．

5 章

p. 102　問 1．N を含む p-シロー群を P とする．任意の p-シロー群は xPx^{-1} で，$N = xNx^{-1} \subset xPx^{-1}$.

p. 103　問 2．N の p-シロー群 P は G の p-シロー群である．G の任意の p-シロー群 $xPx^{-1} \subset xNx^{-1} = N$.

p. 104　問 3．(1) 7-シロー群，13-シロー群ともに1個．

(2) 17-シロー群，19-シロー群ともに1個．

問 4．G の p-シロー群 P の共役の個数 $n_p = 1 + kp | q$ で，$q < p$ ゆえ，$n_p = 1$，∴ $p \lhd G$.

問 5．(1) $S_7 \lhd G$　(2) $S_3 \lhd G$　(3) $S_5 \lhd G$　(4) $S_{11} \lhd G$　(5) S_5 が正規部分群でなければ，S_5 の共役は16個ある．したがって，S_2 は1つ．∴ $S_2 \lhd G$　(6) $S_3 \lhd G$　(7) S_{31} が正規部分群でなければ，S_{31} の共役は32個ある．したがって，S_2 は1つ．∴ $S_2 \lhd G$.

p. 105　問 6．(1) $S_3, S_{11} \lhd G$　(2) $S_7, S_{13} \lhd G$　(3) $S_7, S_{17} \lhd G$

p. 110　問 1．$\mathfrak{S}_3$ の正規鎖は $\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \{e\}$ のみである．これは可換正規鎖であるから，$\mathfrak{S}_3$ は可解である．$\mathfrak{S}_3$ の中心 $Z = \{e\}$ であるから，$\mathfrak{A}_3 \not\subset Z$ で，この列は中心列でない．

p. 111　問 2．H を可解群とし，$H = H_0 \supset H_1 \cdots\cdots \supset H_r = \{e\}$ を可換正規列とする．

かりに N と G/N の巾零性から，G の巾零性がしたがうとすると，H_{r-1}は可換ゆえ，巾零で，H_{r-2}/H_{r-1} も可換ゆえ巾零，したがって H_{r-2} は巾零. こうして，ついには H が巾零群ということになる.

p. 113　問 1.　この場合，どの p-シロー群も正規部分群になるから（p. 113，定理 13 の証明をみよ).

問 2.　有限巾零群のそのシロー群による直積分解を考えよ.

p. 118　問 1.　G が単純群だとすると，S_5 の共役は 16 個あり，$N(S_5)=S_5$. 位数 5^2 の S_5 はアーベル群である.

p. 119　問 2.　問の群 G が単純だとすると，S_{23} の共役は 24 個あることになり，$N(S_{23})$ の位数は $7\cdot 23$，$N(S_{23})/S_{23}$ の位数 7 は $A(S_{23})$ の位数 22 と互いに素である.

p. 120　問 3.　すべての場合，単純だと仮定し，p. 119，定理 17 系を使って矛盾をみちびく. $n_p=p$-シロー群の個数とする.

$g=36$ のとき $n_3=4$	$g=72$ のとき $n_3=4$
$g=2^2\cdot 3^n$ のとき $n_3=4$	$g=2^3\cdot 7^n$ のとき $n_7=8$
$g=108$ のとき $n_3=4$	$g=324$ のとき $n_3=4$
$g=600$ のとき $n_5=6$	$g=648$ のとき $n_3=4$
$g=900$ のとき $n_5=6$	$g=3^3\cdot 5\cdot 7$ のとき $n_3=7$

問 4.　G が単純だとすると，S_5 の共役は 6 か 36. $540\nmid 6!$ であるから，$n_5=36$. $N(S_5)$ の位数は 15. $N(S_5)/S_5$ の位数 3 と S_5 の自己同型群の位数 4 とは互いに素であるから，G は真の正規部分群を含むことになる.

p. 121　問 5.　$K=\mathrm{Ker}\,\pi=\{b|b\in G,\ bx_iN=x_iN\quad \forall i\}=\{b|b\in G,\ b\in x_iNx_i^{-1}\quad \forall i\}=\bigcap xNx^{-1}$，ここで x は G 全体を動く. いま，$K'\lhd G$, $K'\subset N$ とすれば，$K'=xK'x^{-1}\subset xNx^{-1}\quad \forall x\in G\quad \therefore\ K'\subset K$

p. 127　**問題 5**

1.　$H\subset P$ ならば，もちろん $H\subset N(P)$. 逆に，$H\subset N(P)$ ならば，P は $N(P)$ の唯一つの p-シロー群であるから，$H\subset P$.

2.　P の指数 q^n と Q の指数 p^m が互いに素であるから.（p. 46，問 4 をみよ）

3.　(1) $xPx^{-1}=P$ とすれば，$xP^*x^{-1}=xPx^{-1}\cap xNx^{-1}=P^*$ であるから，$N(P)\subset N(P^*)$.

(2)　PN/N の正規化群は $N(PN)/N$ であるから，$N(PN)=N(P)N$ を

示せばよい．$xPNx^{-1}=PN$ とすれば，$xPx^{-1}N=PN$ であるから，$xPx^{-1} \subset PN$. P も xPx^{-1} も $PN=NP$ の p-シロー群であるから，$xPx^{-1}=nyPy^{-1}n^{-1}=nPn^{-1}$, $n\in N$, $y\in P$. $\therefore$ $n^{-1}x\in N(P)$, $x\in NN(P)=N(P)N$. $\therefore$ $N(PN)\subset N(P)N$. 逆に $N(P)N=NN(P)\ni ny$, $n\in N$, $y\in N(P)$ とすれば，$nyPNy^{-1}n^{-1}=nyPy^{-1}Nn^{-1}=nPNn^{-1}=nPN=nNP=NP=PN$. したがって，$N(P)N\subset N(PN)$. $\therefore$ $N(PN)=N(P)N$.

(3) $G\ni x$ に対し xP^*x^{-1} は N の p-シロー群であるから $xP^*x^{-1}=nP^*n^{-1}$, $n\in N$. $\therefore$ $n^{-1}x\in N(P^*)$, $x\in NN(P^*)=N(P^*)N$. ゆえに $N(P^*)N=G$.

4. P の指数は p と素であるから，P の指数と H の指数は互いに素である．したがって，$G=HP=PH$（p. 46，問 4 をみよ）．p. 46，定理 9，系 1 より，$|H:H\cap P|=|HP:P|$ で，これは p と素．$H\cap P$ は H の p-部分群であるから，$H\cap P$ は H の p-シロー群である．

5. $L=xKx^{-1}$, $x\in G$, より $N(L)=xN(K)x^{-1}$. P, xPx^{-1} は $N(L)$ の p-シロー群であるから，$P=uxPx^{-1}u^{-1}$, $u\in N(L)$. $\therefore$ $ux\in N(P)$. また，$(ux)K(ux)^{-1}=uLu^{-1}=L$.

6. 7. p. 105，例題 5 参照.

8. S_{17} の共役の個数は $1+17k$ の形をしていて，15 の約数であるから，1 に等しい．$\therefore$ $S_{17}\lhd G$. ゆえに S_3S_{17}, S_5S_{17} は G の部分群である．$S_3\cap S_{17}$, $S_5\cap S_{17}$ ともに $\{e\}$ であるから，S_3S_{17}, S_5S_{17} の位数はそれぞれ $3\cdot17$, $5\cdot17$ である．S_3 は S_3S_{17} の 3-シロー群であり，$17\not\equiv1 \pmod 3$ であるから，$S_3\lhd S_3S_{17}$. したがって $S_3S_{17}=S_3\otimes S_{17}$. 同様にして，$S_5\lhd S_5S_{17}$ で，$S_5S_{17}=S_5\otimes S_{17}$. つぎに S_3 の G における正規化群は $S_3\otimes S_{17}$ を含み，S_3 の共役の個数 $1+3k$ は $255/(3\times17)=5$ の約数であるから 1 に等しく，$S_3\lhd G$. 同様にして $S_5\lhd G$. したがって $S_3S_5=S_3\otimes S_5\lhd G$. $(S_3\otimes S_5)S_{17}$ は G の部分群で，$(S_3\otimes S_5)\cap S_{17}=\{e\}$ であるから，この部分群の位数は $(3\times5)\times17=255$. $\therefore$ $(S_3\otimes S_5)S_{17}=G$. $S_{17}\lhd G$ であるから，$G=S_3\otimes S_5\otimes S_{17}$. 3 つの直積因子は巡回群であるから，$G$ は巡回群.

9. G は位数 12 の群とする．$S_2\lhd G$ ならば，G/S_2 は巡回群，S_2 はアーベル群であるから，G は可解．$S_2\ntriangleleft G$ のときは S_2 の共役は 3 個ある．このとき $S_3\ntriangleleft G$ とすれば，S_3 の共役は 4 個ある．S_3 の共役と S_2 だけで G 全体になり，S_2 の共役が 3 個あることに反する．したがって，$S_3\lhd G$. $G\rhd$

$S_3 \triangleright \{e\}$ は可換正規鎖であり，G は可解.

G を位数 30 の群とする．$S_5 \triangleleft G$ ならば，G/S_5 は位数 6 の群であって，可解．したがって，G は可解．$S_5 \not\triangleleft G$ のとき，S_5 の共役は 6 個ある．S_5 の共役全体は 25 個の元を含む．したがって位数が 3 の元は 5 個より少ない．S_3 の共役の個数は 1 か 10 であるが，10 ではあり得ない．したがって，$S_3 \triangleleft G$. G/S_3 は位数が 10 であるから可解．したがって，G は可解.

10. G を位数 p^2q の群とする．G の p-シロー群 P が正規部分群ならば，G/P は位数 q の巡回群で，P はアーベル群であるから，G は可解．$P \not\triangleleft G$ のときは，P の共役の個数 $n_p=1+kp=q$ であるから，$q>p$. このとき，q-シロー群 Q が正規部分群でなければ，Q の共役の個数 n_q は p か p^2 かである．$n_q=1+hq$ で $q>p$ ゆえ，$n_q=p^2$. Q とその共役全体で $p^2q-(p^2-1)$ の元を含み，Q とその共役と P とだけで G 全体になり，したがって P の共役が 2 つ以上あることに反する．ゆえに $Q \triangleleft G$. このとき G/Q はアーベル群であるから，G は可解.

11. G を位数 24 の群とする．G の 2-シロー群の共役の個数 n_2 は 1 か 3. 3-シロー群の共役の個数 n_3 は 1 か 4．$n_2=n_3=1$ ならば，$S_2, S_3 \triangleleft G$ で $G=S_2 \otimes S_3$. したがって，G は可解．(位数 8 の S_2 には，p. 112, 例題 3 で示したように，5 つの型があるから，直積 G には，5 つの型がある)．$n_2=3$ のときは，つぎに示すように，2 つの 2-シロー群の共通部分 H は位数 4 の部分群で，$H \triangleleft G$ である．そうすると，$|G:H|=6$ で，G/H は可解．H はアーベル群であるから，G は可解．いま，$P=S_2$ とおく．もう 1 つの 2-シロー群を P' とし，$H=P\cap P'$ の位数を 2^s とおくと，$0 \leqq s \leqq 2$. いま $P \ni a$ で，$aP'a^{-1}=P'$ ならば，P' の共役は 3 個あって，$N(P')=P'$ であるから，$a \in P'$，したがって $a \in P\cap P'$. 逆に $P\cap P' \ni a$ ならば，$aP'a^{-1}=P'$. したがって，P を $H=P\cap P'$ を法として類別して得られる 2^{3-s} 個の各類に対して，P と異なる P の共役が得られる．ゆえに $3-s=1$, $s=2$ であって，H の位数は 4 である．P と P' で生成された群 $\langle P, P'\rangle$ は P より大きく，$|G:P|=3$ であるから，$\langle P, P'\rangle=G$. $H \triangleleft P$, $H \triangleleft P'$ であるから，$H \triangleleft G$.

12. G を位数 $2p$ の群とする．p-シロー群 $P \triangleleft G$. G には位数 2 の元 b が存在する．$P=\langle a\rangle$ で，$P \triangleleft G$ であるから，$bab^{-1}=a^k$. $a=b^2ab^{-2}=a^{k^2}$ であるから，$k^2\equiv 1 \pmod{p}$. $\boldsymbol{Z}_p{}^*$ は巡回群で，この合同式をみたす k は $k\equiv$

$\pm 1 \pmod{p}$ だけである.

(1) $k\equiv 1$ ならば $ab=ba$ で, ab の位数は $2p$, G は巡回群.

(2) $k\equiv -1$ であれば, $bab^{-1}=a^{-1}$ で, G は p 次2面体群である.

13. G を位数 p^n の群, H を位数 p^{n-1} の部分群とすると, p. 113, 補助定理2により, $H\subsetneqq N(H)\subset G$. H の指数は p であるから, $N(H)=G$. $\therefore\ H\lhd G$.

別解　$n=1$ のときは $H=\{e\}$ であって, 明らか. n に関する帰納法で証明する. G の中心を Z とする. $Z\not\subset H$ ならば, $G=ZH$ で, G の元は za, $z\in Z$, $a\in H$, と表され, $zaHa^{-1}z^{-1}=H$ であるから, $H\lhd G$. $Z\subset H$ ならば, $|G/Z|<p^n$ であるから, 帰納法の仮定によって, H/Z は G/Z の, したがって, H は G の正規部分群.

14. $G\supsetneqq Z=Z(G)\supsetneqq\{e\}$ である. p. 112, 例題2より, $|G:Z|=p^2$, $|Z|=p$ となる. G/Z はアーベル群であるから, $Z\supset D(G)$. $Z\supsetneqq D(G)$ ならば, $D(G)=\{e\}$, G はアーベル群となってしまうから, $Z=D(G)$. G/Z はアーベル群であるが, 巡回群でないから, 不変系は (p, p) である.

15. G を位数 $2^3\cdot 7\cdot 11$ の群とし, G は単純でないとすると, 11-シロー群 S_{11} の共役は56個ある. $\therefore N(S_{11})=S_{11}$. S_{11} はアーベル群であるから, p. 118, 定理15系により, G は単純群でないことになって, 矛盾.

16. G を位数 p^2q^2 の群とする. いま, $p<q$ とする. $S_q\lhd G$ であれば, G/S_q, S_q ともにアーベル群であるから, G は可解群である. $S_q\not\lhd G$ とすれば, S_q の共役の個数 $n_q=1+kq$ は p^2 の約数であるから, $n_q=p^2$. したがって, $N(S_q)=S_q$. p. 118, 定理15, 系によって, G は $G=MS_q$, $M\cap S_q=\{e\}$ である正規部分群 M を含む. この M は p-シロー群 S_p である. G/S_p, S_p ともにアーベル群であるから, G は可解.

17. G が単純群であるから, $N(P)\subsetneqq G$. p. 117, 定理15により, $Z(P)\subsetneqq N(P)$. $P\lhd N(P)$ であるから, $N(P)$ の元 a によって, P の自己同型 $\sigma(a): x\longmapsto axa^{-1}$ が引き起こされる. $\sigma(a)$ が恒等写像であるのは, a が P の中心化群に属するとき, その時に限るから $N(P)$ から P の自己同型群 $A(P)$ への準同型 $a\longmapsto\sigma(a)$ の核は $Z(P)$. $A(P)$ の位数は $p-1$ であるから, $|N(P):Z(P)|$ は $p-1$ の約数である.

付　　録

1. 環，体の定義

［定義］　集合 R において，2種類の演算，加法と乗法が定義されていて，つぎの条件がみたされているとき，R は環をつくるという．

1. R は加法に関して可換群（加法群）をつくる．
2. R は乗法に関して閉じている：$R \ni a, b \Longrightarrow ab \in R$
3. R では乗法に関する結合法則が成り立つ：

$$(ab)c = a(bc) \quad \forall a, b, c \in R$$

4. R の任意の元 a, b, c に対して分配法則が成り立つ：

$$(a+b)c = ac + bc, \qquad c(a+b) = ca + cb$$

環 R において，乗法に関して交換法則が成り立つとき，**可換環**という．可換環においては，上の2つの分配法則は同じことである．

環 R の加法群としての単位元0を環の零元という．$a0 = a(0+0) = a0 + a0$, $0a = (0+0)a = 0a + 0a$ であるから，

$$a0 = 0a = 0 \quad \forall a \in R$$

また，つぎの等式が成り立つ．

$$a(-b) = (-a)b = -ab, \qquad (-a)(-b) = ab,$$

$$(a-b)c = ac - bc, \qquad c(a-b) = ca - cb$$

なぜなら，まず，$ab + a(-b) = a\{b + (-b)\} = a0 = 0$ であるから，$a(-b) = -ab$. 同様にして $(-a)b = -ab$ がみちびかれる．さらに，$(-a)(-b) = -(-a)b = -(-ab) = ab$.

つぎに，$(a-b)c = \{a + (-b)\}c = ac + (-b)c = ac + (-bc) = ac - bc$. $c(a-b) = ca - cb$ も同様に出る．

零元0だけでも環をつくる．環 R が0以外の元を含み，乗法に関する単位元，すなわち $ae = ea = a \quad \forall a \in R$ となる元 e を含むとき，e を R の単位元という．単位元は1で表されることがある．

例 1.　整数全体 $\boldsymbol{Z}$ はふつうの加法，乗法に関して，単位元1をもつ可換環をつくる．偶数全体も可換環をつくるが，乗法に関する単位元をもたない．

例 2.　実数を成分にもつ n 次正方行列全体は，行列の加法，乗法に関して非可

換な環をつくる．零元は零行列であり，単位元は単位行列である．

［定義］　環 K において，0以外の元が乗法群をつくるとき，K は**体**をつくるという．乗法に関して交換法則が成り立つ体を**可換体**という．(可換体のことを単に体ということもある)

例 3.　有理数全体 $\boldsymbol{Q}$，実数全体 $\boldsymbol{R}$，複素数全体 $\boldsymbol{C}$ はそれぞれふつうの加法，乗法に関して可換体をつくる．これらをそれぞれ有理数体，実数体，複素数体という．

例 4.　複素数を成分とするつぎの形の2次行列の全体は非可換な体をつくる．

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \quad (\bar{\alpha},\ \bar{\beta}\ \text{は}\ \alpha,\ \beta\ \text{の共役複素数})$$

2.　p 個の元からなる体

2-2-3項で，整数全体 $\boldsymbol{Z}$ を整数 $m>1$ を法として類別したとき，整数 a の属する剰余類を C_a で表すと，m 個の剰余類の全体

$$\boldsymbol{Z}_m = \{C_0, C_1, C_2, \cdots\cdots, C_{m-1}\}$$

は加法 $C_a+C_b=C_{a+b}$ によって加法群をつくること，また $\boldsymbol{Z}_m$ において，乗法を $C_aC_b=C_{ab}$ と定義すれば，

交換法則　$C_aC_b=C_bC_a$

結合法則　$(C_aC_b)C_c=C_a(C_bC_c)$

が成り立つことを述べた．さて，$\boldsymbol{Z}_m \ni C_a, C_b, C_c$ のとき

$$\begin{aligned}(C_a + C_b)C_c &= C_{a+b}C_c = C_{(a+b)c} = C_{ac+bc} \\ &= C_{ac} + C_{bc} = C_aC_c + C_bC_c\end{aligned}$$

であるから，$\boldsymbol{Z}_m$ は可換環をつくる．零元は C_0，C_a のマイナス元 $-C_a=C_{-a}$，単位元は C_1 である．環 $\boldsymbol{Z}_m$ を **m を法とする剰余類環**という．$\boldsymbol{Z}_m$ において零元 C_0 以外の元は必ずしも乗法群をつくるわけではないが，m が素数 p のときは C_0 以外の元 $C_1, C_2, \cdots\cdots, C_{p-1}$ は乗法群，すなわち p を法とする既約剰余類群 $\boldsymbol{Z}_p{}^*$ をつくっている．

［定義］　素数 p を法とする剰余数の全体 $\boldsymbol{Z}_p$ は可換体をつくる．この体は p 個の元からなるいわゆる有限体である．この体を法 p の**剰余類体**という．

3.　正規鎖 $G=G_0 \supset G_1 \supset G_2 \supset \cdots\cdots \supset G_r=\{e\}$ において，$G_0, G_1, G_2, \cdots\cdots, G_r$ はす

べて異なり，G_{i-1} と G_i の間には，これらと異なる G_{i-1} の正規部分群が存在しないとき，すなわち G_{i-1}/G_i がすべて単純群であるとき，この正規鎖を群 G の**組成列**といい，各剰余群を**組成剰余群**という．どの群も組成列をもつとはかぎらないが，有限群は組成列をもつ．すなわち，有限群 G の，G と異なる正規部分群のうち，位数が最大なものを G_1 とし，G_1 と異なる G_1 の正規部分群のうち，位数が最大なものを G_2 とし，これを続ければ，組成列ができる．

つぎの定理は容易に証明できる．

［定理］　有限群が可解群であるための必要十分条件は，その組成列の組成剰余群がすべて位数が素数の巡回群であることである．

組成列をもつ群については，つぎの基本定理が成り立つ．

［定理］　(**ジョルダン・ヘルダー**)

G は組成列をもつ群とし，

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots\cdots \supset G_r = \{e\}$$

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots\cdots \supset H_s = \{e\}$$

を G の2つの組成列とすれば，$r=s$ で，G_{i-1}/G_i と H_{j-1}/H_j は1つずつ適当な順序で同型となる．

このようにして得られる単純群の一定の集合は，群の構成要素として本質的な意味をもち，群はある意味で，これらで合成されていると考えられる．ここに，有限群論の最終の目標であるすべての有限群の分類と関連して，単純群をすべて数えあげるということが問題になってくるわけである．

組成列については，巻末文献〔6〕〔7〕参照．

4. 群の拡大

2つの群 N, F が与えられたとき，N を正規部分群として含む群 G で，$G/N\cong F$ となるようなものをすべて求めること――その可能性とその多様性――は群論における1つの問題である．たとえば，直積 $N\otimes F$ は自明な解である．このような群 G を **N の F による拡大**という．付録3で述べた合成されているというのは，有限群 G の組成列の群 G_i は G_{i+1} の単純群 G_i/G_{i+1} による拡大になっていて，G は，このような単純群による拡大の積み重ねになっているという意味である．

群の拡大については，巻末文献〔3〕,〔6〕,〔9〕参照．

5. 置換表現について

集合 M の変換（M の上の置換ともいう）全体のつくる群 S^M を M の変換群という（1-3節）．とくに n 個の元からなる集合 M の上の置換からなる群（$S^M=\mathfrak{S}_n$ の部分群）を **n 次の置換群**という．

群は，はじめは，代数方程式の根の集合の上の置換群（今日ガロア群とよばれる）として認識されていたので，長い間群の研究はすべて置換群の研究であった．置換群ではその元が特殊であるから，抽象群では表れない特別な現象が見られるので，調べていく上で手掛りがあるわけである．置換群が今日でも研究の重要な対象になっているのは，群の1つの具体的な例を与えているというだけでなく，つぎに示すように，任意の抽象的な有限群に同型な置換群が存在するからである．

［定理］　位数 n の群 G と同型な n 次の置換群が存在する．

［証明］　$G=\{a_1=e,\ a_2,\ \cdots\cdots,\ a_n\}$ とし，G の元 a に対し，

$$\sigma(a)=\begin{pmatrix} a_1 & a_2 & \cdots\cdots & a_n \\ aa_1 & aa_2 & & aa_n \end{pmatrix}=\begin{pmatrix} x \\ ax \end{pmatrix}$$

とおくと，$\sigma(a)\in\mathfrak{S}_n$ である．

$$\sigma(a)\sigma(b)=\begin{pmatrix} bx \\ a(bx) \end{pmatrix}\begin{pmatrix} x \\ bx \end{pmatrix}=\begin{pmatrix} x \\ (ab)x \end{pmatrix}$$

であるから，$\sigma(a)\sigma(b)=\sigma(ab)$．また，$a\neq b$ であれば，$\sigma(a)e=a,\ \sigma(b)e=b$ であるから，$\sigma(a)\neq\sigma(b)$．したがって，$G'=\{\sigma(a)|a\in G\}$ は G と同型である．

一般に群 G から n 次の対称群 $\mathfrak{S}_n$ の中への準同型 φ を G の **n 次の置換表現**という．特に φ が同型のとき，忠実な表現という．上記定理に述べた対応 $\sigma: a\longmapsto\sigma(a)$ は忠実であって，これを G の**左正則表現**という，これは p. 117 に述べた，群 G の部分群 H による置換表現の，$H=\{e\}$ の特別な場合である．

有限群論において，位数が与えられたとき，互いに同型でない群がどれだけ存在するかということは，重要な問題である．任意の整数 $n>0$ に対して，位数 n の巡回群が存在するから，n を位数とする群は少なくとも1つは存在する．この問題は，先の定理によって，$\mathfrak{S}_n$ の互いに同型でない位数 n の部分群をすべて求めることに帰着するが，これがなかなか難しい問題である．n が小さいときはいろいろな具体的方法でこの問題は解決されるが，n が大きくなると，ほとんど絶望的といっていい程，困難さが増してくる．

位数 $n<32$ の群の個数はつぎの表のようになる．

位数：	4	6	8	9	10	12	14	15	16	18
個数：	2	2	5	2	2	5	2	1	14	5

位数：	20	21	22	24	25	26	27	28	30
個数：	5	2	2	15	2	2	5	4	4

位数が素数 p のものは巡回群であるから，上の表から省いてある，位数が p^2 のものはアーベル群で，その不変系が (p^2) のものと (p, p) のものと 2 つある．位数が p^3 のものは 3 つのアーベル群と 2 つの非可換なものがある．巻末文献〔3〕,〔6〕,〔10〕参照．位数が p^4 のものは 5 つのアーベル群と，非可換なものは，$p>2$ のとき 10 個，$p=2$ のときは 9 個ある．巻末文献〔16〕参照．

置換群，置換表現については，巻末文献〔3〕,〔6〕,〔7〕,〔9〕参照．

6. 行列による表現

アーベル群 G の指標――G から，0 でない複素数のつくる群 $\boldsymbol{C}^*$ の中への準同型――の考えを非可換な群に拡張したものとして，群 G から，複素数体 $\boldsymbol{C}$ 上の n 次一般 1 次変換群 $GL(n, \boldsymbol{C}^*)$ の中への準同型 $A: a \longmapsto A(a),\ a \in G$，が考えられる．この準同型を G の行列による**表現**という．

表現論は有限群の研究には欠かせないもので，現在得られている重要な結果のうちには，表現論の助けがなければ，証明が非常に面倒になるとか，または証明できないものが多くある．行列による表現は一般の体の上でも考えられ，とくに素数 p を法とする剰余類体を含むような体の上での表現は重要で，多くの結果が得られている．

行列による表現については，巻末文献〔1〕の第Ⅱ巻，〔3〕の第Ⅱ巻，〔6〕,〔7〕,〔9〕〔14〕〔15〕参照．

7. 体 K 上のベクトル空間

可換体 K の n 個の元の対 $(x_1, x_2, \cdots\cdots, x_n)$ の全体を K^n で表す．

相等 $(x_1, x_2, \cdots\cdots, x_n)=(y_1, y_2, \cdots\cdots, y_n)$ は $x_i=y_i\ \ \forall i$ のとき，そのときに限るとし，K^n の元の和を，

$$(x_1, x_2, \cdots\cdots, x_n)+(y_1, y_2, \cdots\cdots, y_n)$$
$$=(x_1+y_1, x_2+y_2, \cdots\cdots, x_n+y_n)$$

K の元 a と K^n の元の積を，

$$a(x_1, x_2, \cdots\cdots, x_n) = (ax_1, ax_2, \cdots\cdots, ax_n)$$

によって定義すると，つぎのことが成り立つ.

V−1　K^n は加法群をつくる.

V−2　$a(u+v)=au+av,\ \forall a \in K,\ \forall u,\ v \in K^n$

V−3　$(a+b)u=au+bu,\ \forall a,\ b \in K,\ \forall u \in K^n$

V−4　$(ab)u=a(bu),\ \forall a,\ b \in K,\ \forall u \in K^n$

V−5　$1u=u,\ 1 \in K$

一般に，加法群 M があって，1つの体 K の任意の元 a と M の任意の元 u とに対し積 au が M の元として定まり，上記 V−2 から V−5 まで成り立つとき，M を **K 上のベクトル空間**，M の元を**ベクトル**という．とくにベクトル空間 M のどの元も n 個のベクトル $u_1, u_2, \cdots\cdots, u_n$ の1次結合

$$c_1u_1 + c_2u_2 + \cdots\cdots + c_nu_n, \quad c_i \in K$$

と一意的に表されるとき，M は **n 次元**であるという.

K^n は K 上の n 次元ベクトル空間であって，いわゆる線型代数における n 項実数ベクトルの全体 $\boldsymbol{R}^n$ の一般化である．K 上の n 次元ベクトル空間の線型写像（1次変換），線型写像の行列表現などに，実数体 $\boldsymbol{R}$ 上の n 次元ベクトル空間の場合の論法がほとんどすべてそのまま適用される.

集合に関する記号

$a\in A$　または　$A\ni a$	a は A に**含まれる**，A は a を**含む**
	a は A の元である
$a\notin A$　または　$A\not\ni a$	a は A に含まれない
$A\subset B$　または　$B\supset A$	A は B に含まれる，B は A を含む
	A は B の**部分集合**である
$A\not\subset B$　または　$B\not\supset A$	A は B に含まれない
$A\subsetneqq B$　または　$A\subsetneqq B$	A は B の**真の部分集合**である
$A\cap B=\{x\mid x\in A$ かつ $x\in B\}$	A と B の**共通集合**
$A\cap B=\phi$	A と B は共通な元を含まない
	A と B の共通集合は空集合である
$A\cup B=\{x\mid x\in A$ または $x\in B\}$	A と B の**和集合**
$A\times B=\{(a, b)\mid a\in A, b\in B\}$	A と B の**直積**

n 個の集合 $A_1, A_2, \cdots\cdots, A_n$ に対して

$A_1\cap A_2\cap\cdots\cdots\cap A_n$ または $\bigcap_{i=1}^{n}A_i$	$A_1, A_2, \cdots\cdots, A_n$ の共通集合
$A_1\cup A_2\cup\cdots\cdots\cup A_n$ または $\bigcup_{i=1}^{n}A_i$	$A_1, A_2, \cdots\cdots, A_n$ の和集合
$A_1\times A_2\times\cdots\cdots\times A_n=\{(a_1, a_2, \cdots\cdots, a_n)\mid a_i\in A_i(i=1, 2, \cdots\cdots, n)\}$	
	$A_1, A_2, \cdots\cdots, A_n$ の直積

その他の記号

$P \Longrightarrow Q$	P ならば Q, P であるから Q となる等々
$P \Leftrightarrow Q$	P と Q は同値，P は Q であるための必要十分条件
$\forall x\in M$	M の任意の（すべての）元 x に対して
$\forall x, y\in M$	M の任意の元 x, y に対して
$\exists x\in M$	M の中に元 x が存在する

文　　献

代数学の基礎になっているのは群論であり，逆に代数学の知識は群論の研究に欠かせない．代数学を勉強しようとされる方に，第一におすすめできるのはつぎの本である．

〔1〕 B. L. van der Waerden, Algebra I, II, Springer 書店

この本は邦訳（東京図書）があり，英訳もある．第I巻を読めば，代数学の概要を知ることができる．群の表現のことは第II巻にある．

その他

〔2〕 G. Birkhoff・S. MacLane, A Survey of Modern Algebra, Macmilan,（邦訳，白水社）
〔3〕 秋月康夫・鈴木通夫，高等代数学I，II，岩波書店
〔4〕 弥永昌吉・布川正己編，代数学，岩波書店

〔3〕は初学者向きでないが，群論に関しても内容に富んでいる．

群論の書物は数多くあり，すぐれた本が次々と出版されている．日本語の本で，やさしい入門書として

〔5〕 稲葉栄次，群論入門，培風館

がある．群論全般についての標準的な本は

〔6〕 浅野啓三・永尾汎，群論（岩波全書），岩波書店
〔7〕 大島勝，群論，共立出版

〔6〕,〔7〕は内容に多少のちがいがあるが，本書で欠けている点を補い，群論の基本的な知識を身につけるにふさわしい本である．

〔6〕よりややややさしい入門書として，つぎの本もよい．

〔8〕 永尾汎，群論の基礎，基礎数学シリーズ，朝倉書店

数学講座のうちから，群論に関係するものをあげると，

〔9〕 秋月康夫，抽象代数学，基礎数学講座，共立出版
〔10〕 秋月康夫・永田雅宜，抽象代数学，数学演習講座，共立出版
〔11〕 服部昭，現代代数学，近代数学講座，朝倉書店

〔9〕にはたいへんすぐれた群論の解説がある．〔10〕は〔9〕の演習である．〔11〕

は初学者向きでないが，代数学全般にわたり，最近の傾向までとり入れてある．

〔11〕にも，同著書による演習書（同じ講座）がある．

さらに進んだ勉強には，つぎの本がよい．

〔12〕 M. Hall, The theory of groups, Macmilan 書店（邦訳，吉岡書店）

〔13〕 G. W. Curtis·I. Reiner, Representation theory of finite groups and associative algebra, Interscience

〔12〕は通論，〔13〕は表現論である．表現論といえば，つぎの本をおすすめする．

〔14〕 服部昭，群とその表現，共立数学講座，共立出版

〔15〕 J. P. Serre, Représentations linéaries des groupes finis, Hermann 書店（邦訳，岩波書店）

つぎの 2 冊は今日でも参考にされるすぐれた本である．

〔16〕 W. Burnside, Theory of groups of finite order, 1911

〔17〕 Zassenhauss, Lehrbuch der Gruppentheorie, 1937

〔16〕は Dover 書店から再出版され，〔17〕も英訳が Chelsea 書店から出された．

特殊な群の表現論を扱った本としては

〔18〕 弥永昌吉・杉浦光夫，応用数学者のための代数学，岩波書店

〔19〕 山内恭彦・杉浦光夫，連続群論入門，培風館

統計学における配置（デザイン）の理論と有限群との関係を扱ったつぎの本は非常に興味深い．

〔20〕 永尾汎，群とデザイン，数学選書，岩波書店

幾何学的変換，とくに合同変換については，つぎの本がおもしろい．

〔21〕 岩堀長慶，合同変換群の話，現代数学セレクト，現代数学社

有限群論は最近長足の発展をとげ，研究は非常にこまかくなっている．最近の有限群の研究をうかがうために，大変むずかしい本であるが，

〔22〕 伊藤昇，有限群論，現代の数学，共立出版

がある．有限群の研究は専門化の傾向がはげしく，やさしい解説書はとても望めなくなってしまっている現状である．

おわりに，初等整数論の参考書として，つぎの本をあげておく．

〔23〕 高木貞治，初等整数論講義，共立出版

〔24〕 稲葉栄次，整数論，基礎数学講座，共立出版

〔25〕 片山孝次，整数論入門，実教出版

索　　引

さ　行

ま 行

や 行

ら 行

わ 行

著者略歴
森　光弥（もり　みつや）　理学博士
昭和25年　東京大学理学部数学科卒業
昭和29年　武蔵工業大学助教授
昭和41年　津田塾大学教授となり現在にいたる

有限群論入門　NDC 411.63

1975年8月30日　第1刷発行
1980年5月25日　第3刷発行

著　者　森　光　弥
発行者　宇　野　豊　蔵
印　刷　中央印刷株式会社
製　本　株式会社若林製本工場

発行所　実教出版株式会社
東京都千代田区五番町五番地 〒102
電話 東京 (263) 0111 振替 東京 4—183260

定価はカバーに表示してあります
3041－2147-3205